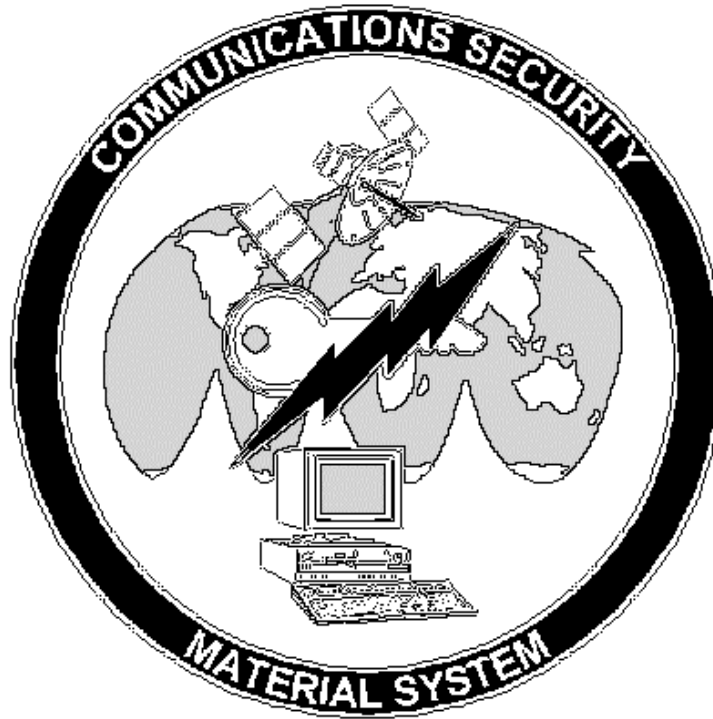


**DIRECTOR,
COMMUNICATIONS SECURITY MATERIAL SYSTEM
NEBRASKA AVENUE COMPLEX
4255 MOUNT VERNON DRIVE SUITE 17337
WASHINGTON DC 20393-5453**

EKMS 3A



ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) INSPECTION MANUAL

SEPTEMBER 2000

**ORIGINAL
(REVERSE BLANK)**



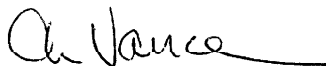
DEPARTMENT OF THE NAVY
COMMUNICATIONS SECURITY MATERIAL SYSTEM
NEBRASKA AVENUE COMPLEX
4255 MOUNT VERNON DRIVE SUITE 17337
WASHINGTON DC 20393-5453

IN REPLY REFER TO:

5040
Ser 80/207
27 OCT 2000

LETTER OF PROMULGATION

1. The Electronic Key Management System Inspection Manual (EKMS 3A), promulgates policy and procedures for conducting EKMS inspections of Department of the Navy (DON), Military Sealift Command and Coast Guard commands, including contracted support personnel. The guidance in this manual is based on policy and procedures set forth in national and Navy COMSEC doctrinal publications.
2. EKMS 3A is effective upon receipt and replaces all previously issued and dated EKMS inspection guidance.
3. EKMS 3A is authorized for reproduction and use in any operational environment.


C. L. VANCE

LIST OF EFFECTIVE PAGESPAGE NUMBEREFFECTIVE PAGES

FRONT COVER (REVERSE BLANK) (unnumbered)	ORIGINAL
I (REVERSE BLANK)	ORIGINAL
III (REVERSE BLANK)	ORIGINAL
V (REVERSE BLANK)	ORIGINAL
VII (REVERSE BLANK)	ORIGINAL
IX THRU XI (REVERSE BLANK)	ORIGINAL
1-1 thru 1-4	ORIGINAL
2-1 thru 2-5 (REVERSE BLANK)	ORIGINAL
3-1 thru 3-3 (REVERSE BLANK)	ORIGINAL
4-1 thru 4-3 (REVERSE BLANK)	ORIGINAL
A-1 (REVERSE BLANK) thru A-52	ORIGINAL
B-1 (REVERSE BLANK)	ORIGINAL
B-3 (REVERSE BLANK) thru B-31 (REVERSE BLANK)	ORIGINAL
C-1 (REVERSE BLANK)	ORIGINAL
C-3 (REVERSE BLANK) thru C-28	ORIGINAL
D-1 (REVERSE BLANK) thru D-7 (REVERSE BLANK)	ORIGINAL
E-1 (REVERSE BLANK) thru E-7 (REVERSE BLANK)	ORIGINAL
F-1 thru F-2	ORIGINAL
G-1 (REVERSE BLANK)	ORIGINAL
BACK COVER (REVERSE BLANK) (unnumbered)	ORIGINAL

TABLE OF CONTENTS

**CHAPTER 1 -- INTRODUCTION TO THE ELECTRONIC KEY MANAGEMENT SYSTEM
(EKMS) INSPECTION/AUDIT PROGRAM**

- 101. Purpose
- 105. Scope and Application
 - a. Source
 - b. Scope
 - c. Application
 - d. Recommendations
- 110. Definitions
 - a. Audit/Inspection
 - b. EKMS Training Visit
 - c. Electronic Key Management System (EKMS)
 - d. Communications Security (COMSEC)
 - e. Follow-up
 - f. Physical Security Inspection
 - g. Physical Security Survey
- 115. Responsibility
 - a. Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM)
 - b. Director, Communications Security Material System (DCMS)
 - c. Immediate Superior in Command/Immediate Unit Commander (ISIC/IUC)
 - d. EKMS Inspection Team Leader
 - e. EKMS Inspection Team Member
- 120. Special Notes
 - a. EKMS Manager
 - b. Local Element

TABLE OF CONTENTS (CONT'D)

CHAPTER 2 -- EKMS INSPECTION POLICY AND PROCEDURES

- 201. General Policy
- 205. EKMS Inspection Process
 - a. EKMS Inspection
 - b. Preinspection Guidelines
 - c. Approval of COMSEC Facilities
 - d. Evaluation Criteria
 - e. Re-inspection

CHAPTER 3 -- ASSIGNMENT OF EKMS INSPECTORS

- 301. Designation Requirements for EKMS Inspectors
- 305. Recommendation for Assignment
- 310. EKMS Inspector Assistance

CHAPTER 4 -- EKMS INSPECTION REPORTING PROCEDURES

- 401. Content and Submission Guidelines
- 405. EKMS Feedback Report
- 410. Privileged Nature of Inspection Reports

LIST OF ANNEXES

- ANNEX A: EKMS INSPECTION GUIDE, EKMS MANAGER
- ANNEX B: EKMS INSPECTION GUIDE, LOCAL ELEMENT (ISSUING)
- ANNEX C: EKMS INSPECTION GUIDE, LOCAL ELEMENT (USING)
- ANNEX D: INSPECTION GUIDE, VAULT
- ANNEX E: INSPECTION GUIDE, FIXED COMSEC FACILITIES

TABLE OF CONTENTS (CONT'D)

ANNEX F: EKMS INSPECTION REPORT EXAMPLE

ANNEX G: EKMS FEEDBACK REPORT EXAMPLE

[101]

CHAPTER 1 - INTRODUCTION TO THE ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) INSPECTION/AUDIT PROGRAM

101. PURPOSE. This manual prescribes policies and procedures related to conducting formal Communications Security (COMSEC) inspections of Electronic Key Management System (EKMS) accounts within the Department of the Navy (DON), including U.S. Navy, Military Sealift Command (MSC), Marine Corps, Coast Guard (COGARD), and contracted support personnel. Annexes A through F pertain.

105. SCOPE AND APPLICATION:

a. **Source.** The policies and procedures in this manual are derived from National, Department of Defense (DOD), and DON COMSEC doctrine.

b. **Scope.** EKMS 3A establishes qualification standards for EKMS Inspectors and prescribes the minimum standards for conducting EKMS inspections. Additional unique requirements may be imposed by the Commandant of the Marine Corps (CMC CPIA), COGARD Telecommunications Information Systems Command (TISCOM ISD-3B), Fleet Commanders-in-Chief (FLTCINC), Type Commanders (TYCOM), Immediate Superiors in Command (ISIC), and Immediate Unit Commanders (IUC) for supported commands, units and activities.

c. **Application.** The COMSEC requirements in this manual apply to all DON and Coast Guard activities maintaining a numbered EKMS account which use EKMS. The EKMS inspection policies and procedures apply to all DON and Coast Guard ISICs/IUCs whose subordinate activities maintain a numbered EKMS account.

d. **Recommendations.** Recommended changes to this instruction will be submitted to Director, Communications Security Material System (DCMS), EKMS Education and Training Department (80), via the administrative chain of command.

110. DEFINITIONS:

a. **Audit/Inspection.** A formal, independent review and examination of records and activities conducted to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

The examination must be conducted by an authority from a different organization than that of the inspected facility. The examination must be concluded with a follow up to recommend necessary changes in controls, policies, or procedures.

b. **EKMS Training Visit**. On-site refresher training (not to be used in lieu of the unannounced biennial EKMS inspection) in the management and handling of COMSEC material. An EKMS training visit is required for each Marine Corps and Coast Guard numbered EKMS account serviced by DCMS (military and civilian) every 18 months. EKMS training visits are optional for Navy numbered EKMS accounts.

c. **Electronic Key Management System (EKMS)**. The logistics and accounting system through which electronic key is accounted, distributed, generated, controlled, destroyed and safeguarded. It also provides management of physical key and non-key COMSEC-related items.

d. **Communications Security (COMSEC)**. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning National security; protective measures taken to ensure the authenticity of such telecommunications.

e. **Follow-up**. The process of ensuring that a command is taking adequate action on approved recommendations contained in an inspection report. This action is normally accomplished by a follow-up letter report.

f. **Physical Security Inspection**. An examination by a certified inspector of an activity's physical security and loss prevention programs to determine compliance with physical security policy. Annexes D and E pertain. Categories of inspections include:

(1) **Navy and Military Sealift Command**. A physical security inspection is normally conducted by the ISIC. Follow-up action to correct noted deficiencies is required.

(2) **Marine Corps**. Physical security inspections are normally conducted as part of the command inspection program. Commanding Officers will establish local physical security inspection programs for their subordinate commands.

[110]

(3) Coast Guard. A specific, on-site examination of any facility or activity conducted by authorized COMSEC or physical security personnel to determine vulnerabilities and compliance with physical security policies as established in COMDTINST 5530.1 (series).

g. Physical Security Survey. An evaluation of the overall security posture of a given facility or activity. The survey should not be regarded as an inspection or investigation. Physical security surveys will be completed using NAVMC 11121. At the discretion of the Commanding Officer, the completed NAVMC 11121 may be used as part of the physical security inspection.

NOTE: Marine Corps - a specific, on-site examination of any facility or activity conducted by a trained physical security specialist (MOS 5814) to identify security weaknesses and recommend corrective measures.)

115. RESPONSIBILITY:

a. Commander, Naval Computer and Telecommunications Command (CNCTC). CNCTC implemented the EKMS inspection program for the DON and U.S. Coast Guard.

b. Director, Communications Security Material System (DCMS). DCMS administers the EKMS inspection program for the DON and the Coast Guard.

c. Immediate Superior in Command/Immediate Unit Commander (ISIC/IUC). The ISIC/IUC is responsible for conducting required EKMS inspections (Annexes A through C) and facility approvals (Annexes D and E) for their subordinate commands. Within the Marine Corps, the ISIC is the command which has administrative control over a unit.

d. EKMS Inspection Team Leader. The senior certified EKMS inspector assigned to and in charge of the EKMS inspection team. The EKMS Inspection Leader is responsible to the ISIC/IUC for the proper conduct and reporting of the EKMS inspection in accordance with this instruction and supplementary guidance provided by the ISIC/IUC.

e. EKMS Inspection Team Member. The EKMS Inspection Team Member, if assigned/tasked, is responsible to the EKMS Inspection Team Leader for properly conducting that portion of the EKMS inspection assigned. All significant discrepancies identified by

an EKMS Inspection Team Member will be validated by the EKMS Inspection Team Leader.

120. SPECIAL NOTES:

a. **Electronic Key Management System (EKMS) Manager.** The term, CMS Custodian, used in other instructions, has been replaced by the new term EKMS Manager to reflect the additional duties required.

b. **Local Element (LE).** The term, Local Element, applies where either the term Local Holder or CMS User were used in other instructions.

[201]

CHAPTER 2 - EKMS INSPECTION POLICY AND PROCEDURES

201. GENERAL POLICY: ISICs/IUCs must conduct unannounced EKMS inspections of their subordinate commands and units once every 24 months (biennially). ISICs/IUCs are also responsible for initial physical security facility approval and recertification for COMSEC material storage. EKMS inspections shall be performed only by personnel who meet the designation requirements in Article 301 of this manual.

NOTE: Within the Marine Corps, the inspected command will provide the EKMS inspector with a copy of the most recent physical security survey to be used as a basis for initial physical security facility approval and recertification.

205. EKMS INSPECTION PROCESS:

a. **EKMS inspection.** The EKMS inspection must be conducted in detail to evaluate the safeguarding, accounting and disposition of COMSEC material within a COMSEC account. An inspection will include the Local Account and all Local Element(s) (LEs). The inspection checklists, contained in Annexes A through E, will be used as inspection guidelines. Specifically, Annexes A through C address required, as applicable, EKMS inspector checklists; whereas, Annexes D and E address ISIC required actions that may, or may not, be included as part of the EKMS inspection process. CMC, COGARD TISCOM, MSC, FLTCINCs, TYCOMs and ISICs/IUCs may supplement Annexes A through E with additional, unique requirements. Additional requirements incorporated into the inspection guides must contain references of source documents that reflect the most current COMSEC policy and procedures. EKMS Managers who are also designated EKMS Inspectors are not authorized to conduct formal EKMS inspections on their own accounts or their LEs; however, they may conduct spot-checks at their discretion.

NOTES:

1. If there are a large number of LEs that are external to the command, a minimum of three must be included.
2. LEs which are not collocated within a 50 mile radius of the inspected command may be exempted from the inspection at the discretion of the inspecting command.

The EKMS inspection process is an excellent tool to assess command COMSEC handling procedures and improve the way we do business. The inspected commands are the customer of the EKMS

Inspector. These commands want to do a good job, so it follows that weak areas may be attributed to factors which make it more difficult to do quality work. The EKMS Inspector is tasked with identifying and analyzing those factors and offering suggestions for improvement. The goal for the EKMS Inspector should be to help improve the abilities of those who do the work to better accomplish their mission. The purpose of the EKMS inspection is not to punish a command by catching them doing something wrong, but to identify those areas that need to be improved in order for that command to operate in the most effective and efficient manner.

b. **Preinspection Guidelines.** Prior to conducting an EKMS inspection, the inspector(s) should:

(1) Become familiar with other available regulations and directives of higher authority that apply to the command or unit to be inspected.

(2) Research the most recent history on the management of the EKMS account to include:

(a) previous EKMS/CMS inspections;

(b) documentation of problem conditions identified and corrective actions recommended/taken; and,

(c) information regarding reports of COMSEC incidents or insecurities.

(3) Review areas of special interest identified by DCMS, ISIC/IUC or higher authority.

c. **Approval of COMSEC Facilities.** Standards for safeguarding COMSEC facilities are necessary to ensure the integrity of the classified COMSEC material contained therein. Each COMSEC facility must meet minimum physical security standards and must be approved by the responsible department or agency (e.g., ISIC, IUC) to hold classified COMSEC material prior to its use. The responsible department or agency of the Local Account is that account's ISIC or IUC. For a LE whose command is different from the Local Account, the LE's ISIC or IUC will conduct the COMSEC facilities approval of that account or user facility. This approval should be based upon a physical security inspection that determines whether or not the COMSEC facility meets the physical safeguarding standards outlined in DON/Coast

[205]

Guard COMSEC security manuals and CMS 21(Series). This physical security inspection should be performed by a qualified physical security officer. After the initial approval, the COMSEC facility will be reinspected at intervals no greater than 24 months. This reinspection may be completed in conjunction with the unannounced EKMS inspection. The COMSEC facility must also be reinspected and approval confirmed when there is evidence of penetration or tampering, after alterations that significantly change the physical characteristics of the facility, when the facility is relocated, or when it is re-occupied after being temporarily abandoned.

NOTE: A Letter or Memorandum of Agreement (LOA/MOA) between the Local Account and the Local Element may stipulate that the Local Account ISIC can certify and/or recertify COMSEC facilities.

d. **Evaluation Criteria.** Upon completion of the inspection, an evaluation of either Satisfactory or Unsatisfactory will be assigned. The following minimum standards must be used to evaluate inspection results as unsatisfactory:

(1) One (1) COMSEC Incident. (Incidents identified by the inspector during the course of inspection.)

or

(2) Three (3) Practices Dangerous to Security (PDS). (Includes Reportable and Non-reportable PDS's identified by the inspector during course of inspection.)

or

(3) Major administrative errors that exceed: (Inspector must obtain total line items from the most current DCMS generated Fixed Cycle Inventory):

(a) for accounts up to and including 120 line items, maximum of 10 errors.

(b) for accounts between 121 and 250 line items, maximum of 20 errors.

(c) for accounts between 251 and 400 line items, maximum of 30 errors.

(d) for accounts between 401 and 500 line items, maximum of 35 errors.

(e) for accounts of 500 line items or greater, maximum of 40 errors.

NOTE: During the review of the administrative process, inspectors should also attempt to identify trends of common repetitive errors (e.g., repeatedly missing initials on line-outs). Repetitive administrative errors should be graded as one error. Major administrative errors are those that are considered significantly important enough to require action. A repetitive administrative error is considered a major error. Minor administrative errors, not repetitive in nature, should not be considered a major error when evaluating the above inspection criteria.

(4) Inspectors shall include the overall performance of the EKMS account along with the number and description of any insecurities, PDS, and/or major administrative errors in the inspection report.

(5) The biennial inspection performed by the ISIC is the only authorized, formal EKMS inspection. No other entities will conduct COMSEC inspections.

e. **Re-Inspection.** If an account being inspected receives a grade of Unsatisfactory on an EKMS inspection or fails certification/recertification:

(1) An EKMS re-inspection will be conducted at the discretion of the ISIC but no later than three (3) months from the date of failure.

(2) Certification/Recertification failure:

(a) Certification - The COMSEC facility must be modified to meet specifications and be reinspected.

(b) Recertification - Account must comply with waiver requirements as set forth in OPNAVINST 5530.14C Appendix IV.

[205]

NOTE: Per OPNAVINST 5530.14C Appendix IV, approved waivers will exempt the recipient from a specific security standard for 12 months. Repairs should be effected as soon as possible, and the COMSEC facility will be reinspected. For Naval facilities, waiver requests must be forwarded to CNO (N-09N), information copy to DCMS//20//, in order to continue to hold COMSEC material.

[301]

CHAPTER 3 - ASSIGNMENT OF EKMS INSPECTORS

301. DESIGNATION REQUIREMENTS FOR EKMS INSPECTORS. ISICs/IUCs must ensure that their personnel meet the following minimum requirements prior to assigning them as EKMS Inspectors:

- a. U.S. citizen (immigrant aliens are not eligible).
- b. Possess a Top Secret clearance.
- c. Inspection Team Leaders must be E-7 (E-6 for Marine Corps, GS-7 for Civilian Government Service employees) or higher.

NOTE: Submit request for waivers to Team Leader minimum grade requirements to DCMS Washington DC//80//.

- d. Inspection Team Members must be E-6 (GS-7 for Civilian Government Service employees) or higher.
- e. Inspection Team Leaders must have previously served as an EKMS Manager or CMS Custodian or alternate for at least six months within the past 36 months.
- f. Team Members must have served at least as CMS users and should be thoroughly knowledgeable of CMS policies and procedures.
- g. All EKMS Inspectors must successfully complete the EKMS Manager Course of Instruction (V-4C-0013) within the previous 36 months. (Optional for recertification as an EKMS Inspector, at the discretion of the ISIC.)

h. Attend a classroom EKMS Inspector Training Seminar conducted by one of the CMS Advice and Assistance (A&A) Teams as listed in CMS 21(Series).

i. Within 30 days after completing the EKMS Inspector Training Seminar:

(1) Assist with a minimum of one EKMS A&A training visit.

(2) Participate in an actual EKMS inspection with a qualified EKMS Inspector. This requirement is waived for the recertification of current EKMS inspectors.

NOTE: In addition to the requirements outlined in Article 301 with the exception of sub paragraph i.(2), the following information is applicable for U.S. Coast Guard ISIC inspectors:

1. U.S. Coast Guard Area/District personnel who have been identified for appointment as an ISIC inspector, after completion of the above requirements, must participate in an actual EKMS inspection with U.S. Coast Guard TISCOM Chief, Secure Communications Services Branch (ISD-3B) as the final step in the inspection certification process.

305. RECOMMENDATION FOR ASSIGNMENT. Upon favorable completion of the requirements in Article 301, the A&A team providing required training will submit a recommendation to DCMS. DCMS will forward a letter of certification recommending assignment as an EKMS Inspector to the individual's command. The command will then appoint the inspector in writing. In order for an EKMS Inspector to retain their certification, personnel must re-attend the EKMS Inspector Training Seminar under the following situations:

- a. Every 36 months while assigned as an EKMS Inspector.
- b. Personnel re-assigned as an EKMS Inspector that have been out of the program for a period exceeding 12 months, providing all remaining requirements remain valid.
- c. Additional training, as directed.

Upon completion of a subsequent EKMS Inspector Training Seminar, DCMS will forward a letter of recommendation for continued assignment as an EKMS Inspector to the individual's command.

Note: U.S. Coast Guard personnel who have favorably completed the requirements of Article 301, after a recommendation has been forwarded to DCMS by TISCOM(ISD-3B), TISCOM(ISD-3B) will issue an EKMS Inspector Certificate to the individual's command which authorizes appointment of the individual as an EKMS Inspector.

[310]

310. EKMS INSPECTOR ASSISTANCE. An ISIC/IUC may require the assistance of an EKMS Inspector due to the unavailability of a qualified EKMS Inspector on staff. ISIC's shall first request assistance from the next senior in command. If an inspector is not available, further requests for assistance may be forwarded to DCMS WASHINGTON DC//80//. Requests should be submitted 90 days prior to the inspection date to facilitate scheduling. DCMS will identify qualified EKMS Inspectors in the geographical area concerned and coordinate, as needed. The assigned EKMS Inspector(s) will conduct the EKMS inspection for and under the authority of the requesting ISIC/IUC. The ISIC should assist the assigned EKMS Inspector in obtaining any unique supplemental requirements which apply to the inspected command as outlined in Article 205. Any expenses incurred by the assigned EKMS Inspector, and/or supported personnel, will be the responsibility of the requesting ISIC/IUC.

CHAPTER 4 - EKMS INSPECTION REPORTING PROCEDURES**401. CONTENT AND SUBMISSION GUIDELINES:**

a. Significant deficiencies disclosed by the inspecting officials which appear to require action by higher level authorities must be reported immediately to the Commanding Officer (CO) of the inspected command.

b. An informal out-brief must be provided by the EKMS Inspector to the Commanding Officer, Officer-In-Charge (OIC), or Staff CMS Responsibility Officer (SCMSRO) at the conclusion of the inspection.

c. Formal EKMS inspection reports evaluated as unsatisfactory in accordance with Chapter 2 must provide references and comments to substantiate the evaluation. All formal EKMS inspection reports must contain recommendations for correcting deficiencies. (See Annex F for an example of an EKMS inspection report.)

d. Approval to continue to hold classified COMSEC material must be included in the inspection report.

e. Formal EKMS inspection reports will be submitted by the EKMS Inspector to the ISIC for endorsement and forwarding to the inspected command. The endorsement will direct the inspected command to correct the deficiencies and return a report of corrective measures within the timeframe determined by the ISIC/IUC. EKMS Inspectors inspecting Echelon Two EKMS accounts will submit inspection reports to DCMS (80). Do not forward copies of inspection reports from other commands to DCMS, unless directed.

405. EKMS FEEDBACK REPORT. Feedback is an important management tool. Submit feedback reports regarding significant discrepancies or misinterpretations of COMSEC policies or procedures to DCMS with information copy to CNCTC and the Chain of Command. ISIC/IUCs are encouraged to forward such information to improve not only the EKMS inspection program but to improve the COMSEC system as a whole. The use of this report is strongly encouraged as it can provide DCMS with information, practices, or procedures which may be applied advantageously throughout the DON and Coast Guard EKMS communities. Annex G provides an example of a EKMS feedback report message.

410. PRIVILEGED NATURE OF INSPECTION REPORTS. Release of EKMS Inspection reports prepared under the provision of this manual require appropriate restrictions on public access and access by governmental organizations external to the DON. Inspectors serve as the ISIC's representative for evaluating the EKMS account management of subordinate commands. The release of reports outside the original distribution as designated by the ISIC would inhibit the exchange of full and open views between the inspector and those being inspected and would seriously impair the effectiveness of this management tool. In addition to being marked FOR OFFICIAL USE ONLY, the following caveat shall be included on all EKMS Inspection reports:

a. **Navy.** "The information contained in this report relates to the internal practices of the Department of the Navy. This document is therefore an internal communication. This report is not releasable, nor may its contents be disclosed outside the Department of the Navy without prior approval. This report may not be reproduced, in whole or in part, without approval from an appropriate superior authority. In accordance with this instruction and other related regulations, requests for, or correspondence related to this report coming from outside sources shall be promptly referred to the proper authority. The reviewing authority shall in turn refer the request, with recommended actions, to the appropriate Fleet Commander-in-Chief. Holders of this report shall strictly observe these restrictions."

b. **Marine Corps.** "The information contained herein relates to the internal practices of the Department of the Navy and the U.S. Marine Corps. This report is not releasable, nor may its contents be disclosed in whole or in part, without prior approval of (the inspecting command), CMC or DCMS (80). In accordance with this instruction, requests for this report, portions thereof, or correspondence related thereto, from a source external to the Department of the Navy shall be promptly referred to CMC Communications Security Branch (CPA). Holders of this report shall strictly observe this caveat."

c. **Coast Guard.** "The information contained herein relates to the internal practices of the Department of Transportation and is an internal communication within the inspecting command. This report of (inspecting authority) is not releasable, nor may its contents be disclosed outside of original distribution, nor may it be reproduced in whole or in part, without prior approval of (inspecting authority), COGARD TISCOM, or DCMS (80). In accordance with this instruction, requests for this report,

[410]

portions thereof, or correspondence related thereto, from a source external to the Department of Transportation shall be promptly referred to (inspecting authority) who shall further refer the request with recommended action thereon to the Commander, U.S. Coast Guard Telecommunications Information Systems Command (COGARD TISCOM, ISD-3B). Holders of this report shall strictly observe this caveat."

<p align="center"> ANNEX A EKMS INSPECTION GUIDE EKMS MANAGER </p>

PURPOSE. The purpose of this inspection guide is to ensure all aspects of COMSEC management are covered by the EKMS inspectors during the account inspection.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

Immediate Superior in Command (if other than EKMS Inspector)
of Unit Inspected: _____

Date of Last Inspection: _____

Name/Grade/Rate and Command of EKMS Inspector:

Date of Last Facilities Approval: _____

EKMS Manager Name/Grade: _____

Alternate EKMS Manager Name/Grade:

Identify Following, as Applicable/Assigned:

Second Alternate EKMS Manager Name/Grade:

Third Alternate EKMS Manager Name/Grade:

Account Clerk Name/Grade: _____

<p style="text-align: center;">ANNEX A EKMS INSPECTION GUIDE EKMS MANAGER</p>
--

SECTION IDENTIFICATION

- 1 - Security
- 2 - EKMS Manager Responsibilities
- 3 - Account Clerk
- 4 - LCMS/NEAT/CARS
- 5 - Chronological File
- 6 - Transaction Status Log
- 7 - COMSEC Material Receipts/Transfers
- 8 - Destruction Procedures/Reports
- 9 - DCMS-Generated Fixed Cycle (FC) Inventory Reports
- 10 - Combined/Special DCMS-Generated Inventory Reports
- 11 - Completing SF-153 Inventory Reports
- 12 - Correspondence, Message, and Directives File
- 13 - COMSEC Library
- 14 - General Message File (GMF)
- 15 - Local Custody File
- 16 - Report Retention/Disposition
- 17 - Resealing/Status Markings
- 18 - Pagechecks

<p>ANNEX A EKMS INSPECTION GUIDE EKMS MANAGER</p>
--

SECTION IDENTIFICATION (CONT'D)

- 19 - Corrections and Amendments
- 20 - STU-III
- 21 - Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer (OTAT)
- 22 - Data Transfer Device (DTD)
- 23 - Emergency Protection of COMSEC Material
- 24 - Emergency Destruction Plan (EDP)
- 25 - Commanding Officer (CO, OIC, SCMSRO) Responsibilities
- 26 - Material Accountability Tracking

<p style="text-align: center;">ANNEX A EKMS INSPECTION GUIDE EKMS MANAGER</p>
--

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the EKMS Inspector conducting the inspection. Per Chapter 2 and Article 401.c., inspection reports evaluated as unsatisfactory must include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to annotate comments to any question that receives a negative response. This inclusion in the inspection checklists should greatly aid inspectors and commands when conducting the out-brief and writing the official report of inspection results.

SECTION 1 -- SECURITY

NOTE: Inspect COMSEC vault using Annex D or E as appropriate

YES	NO	
_____	_____	<p>1. Are adequate visitor controls enforced to ensure that access to classified information is given only to visitors who possess the proper identification, security clearance, and NEED TO KNOW? [SECNAVINST 5510.30A, Article 11-1 paragraph 2,3; SECNAVINST 5510.36, Article 7-11; CMS 21A, Article 550.e]</p> <p>_____</p>
_____	_____	<p>2. Is a visitor's register maintained and retained for one year from the date the register was completed? [CMS 21A, Article 550.e; Annex T]</p> <p>_____</p>
_____	_____	<p>3. Is unescorted access limited to individuals whose duties require such access and who meet access requirements? [CMS 21A, Articles 505, 535, 550.e]</p> <p>_____</p>

ANNEX ASECTION 1 -- SECURITY (CONT'D)

YES

NO

- | | | |
|--|-------|---|
| <hr/> | <hr/> | 4. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list? [CMS 21A, Article 550.e] |
| <hr/> | | |
| <hr/> | <hr/> | 5. <u>PART A:</u> Are personnel whose duties require access to COMSEC material formally authorized in writing by the CO? [CMS 21A, Article 450.C and 505.d] |
| <hr/> | | |
| <hr/> | <hr/> | <u>PART B:</u> If personnel are authorized access to COMSEC material on an access list, has the list been updated annually or whenever the status of an individual changed? [CMS 21A, Article 505.d(2)] |
| <hr/> | | |
| <hr/> | <hr/> | 6. Do all personnel having access to COMSEC material have a clearance equal to or greater than the highest classification of the material? [CMS 21A, Article 505.a] |
|
<u>NOTE:</u> LMD/KP System Administrator's and Operator's must have a minimum clearance level of SECRET. | | |
| <hr/> | | |

ANNEX A

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	<p>7. Is security clearance data of personnel whose duties require access to COMSEC material maintained by the Command Security Manager? [SECNAVINST 5510.30A, Article 9-5 paragraphs 2,3,4,5]</p> <p>NOTE: For Marine Corps, documented in the Marine Corps Total Force System (MCTFS). For Coast Guard, documented in the Personnel Management Information System (PMIS).</p>
_____	_____	<p>8. Has formal facility approval been given in writing, by ISIC or higher authority, to hold classified COMSEC material? [CMS 21A, Article 405.a(2), 405.g(2) and 550.d(1)]</p>
_____	_____	<p>9. Is the exterior of each COMSEC security container free of markings which reveal the classification of the material stored therein? [SECNAVINST 5510.36, Article 10-1, paragraph 3]</p>
_____	_____	<p>10. Is the space/compartment or vault which contains COMSEC material outwardly identified as "RESTRICTED AREA"? [OPNAVINST 5530.14C, Article 0319.d, Appendixes VI, VII]</p>
_____	_____	<p>11. Are applicable security controls (e.g., guards and alarms) in place in accordance with SECNAVINST 5510.36, Chapter 10? [CMS 21A, Article 520.a(3)]</p>

ANNEX A

SECTION 1 -- SECURITY (CONT'D)

YES

NO

_____ 12. Do storage containers meet the minimum security requirements for the highest classification of keying material stored therein? [CMS 21A, Article 520.c, 520.d and 520.e; SECNAVINST 5510.36, Chapter 10]

NOTE: Effective 14 April 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any classified material. [CMS 21A, Article 520.f]

_____ 13. Is a Maintenance Record for Security Containers and Vault Doors (Optional Form 89) maintained for each security container and retained within the container? [SECNAVINST 5510.36, Article 10-15, paragraph 3, Exhibit 10C; CMS 21A, Article 520.b(3)]

_____ 14. Are all damages, repairs or alterations to the container or parts of the container (e.g., Group 1R locks, locking drawer, drawer head, etc.) properly documented on an Optional Form 89? [SECNAVINST 5510.36, Article 10-15, paragraph 3; CMS 21A, Article 520.b(3)]

_____ 15. Do storage containers conform to the two-person integrity (TPI) requirements for the protection of Top Secret COMSEC keying material? [CMS 21A, Article 520.e]

ANNEX A

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	16. Is a Security Container Information Form (SF 700) maintained for each lock combination and placed in each COMSEC security container? [SECNAVINST 5510.36, Article 10-12, paragraph 3; CMS 21A, Article 520.b(1)] _____
_____	_____	17. Is a Security Container Check Sheet (SF-702) maintained for each lock combination of a COMSEC storage container? [SECNAVINST 5510.36, Article 7-10; CMS 21A, Article 520.b(2)] _____
_____	_____	18. Except in an emergency, are combinations to the COMSEC Account vault/security containers restricted to the EKMS Manager and Alternates only? [CMS 21A, Article 515.c(1)] _____
_____	_____	19. If the COMSEC facility is continuously manned, are security checks conducted at least once every 24 hours? [CMS 21A, Article 550.d(3)(a)] NOTE: Recorded in accordance with local command directive (e.g. line item on watch-to-watch inventory or SF-701) _____
_____	_____	20. In a non-continuously manned COMSEC facility, are security checks conducted prior to departure of the last person and documented using the Activity Security Checklist (SF-701)? [CMS 21A, Article 550.d(3)(b); SECNAVINST 5510.36, Article 7-10] _____

ANNEX A

SECTION 1 -- SECURITY (CONT'D)

YES

NO

_____ 21. If a COMSEC facility is in a high risk area and unmanned for periods greater than 24 hours, is a check conducted at least once every 24 hours to ensure that all doors are locked and that there have been no attempts at forceful entry. [CMS 21A, Article 550.d(3)(c)]

NOTE: Recorded in accordance with local command directive (e.g. annotated on SF-702)

_____ 22. Does any one person have knowledge of both combinations to any one TPI container? [CMS 21A, Article 515.c(2)]

NOTE: A "Yes" answer on this question constitutes non-compliance. A "No" answer on this question constitutes compliance.

_____ 23. Are all sealed records of combinations to COMSEC containers maintained in an approved security container (other than the container where the COMSEC material is stored), and available to duty personnel for emergency use? [CMS 21A, Article 515.e]

_____ 24. Are combinations to COMSEC containers changed when initially placed in use, taken out of service, upon transfer/reassignment of personnel who have access, or when compromised? [SECNAVINST 5510.36, Article 10-12; CMS 21A, Article 515.b]

ANNEX A

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
		25. Is each COMSEC security container record of combination protected as follows: [CMS 21A, Article 515.f]
_____	_____	a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope? _____
_____	_____	b. Combination envelope sealed using transparent lamination or plastic tape? _____
_____	_____	c. Name(s) and address(es) of individual(s) authorized access to the combination recorded on the front of the envelope? _____
_____	_____	d. Proper classification markings on envelope? [CMS 21A, Article 515.d] _____
_____	_____	e. Are the envelopes inspected monthly to ensure they have not been tampered with? _____
_____	_____	26. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and segregated by status, type and classification? (Example: Effective, Secret keymat <u>not</u> stored with superseded, Secret keymat or effective, Top Secret keymat <u>not</u> stored with effective, Confidential keymat.) [CMS 21A, Article 520.a(4); Annex M, paragraph 3.b] _____

ANNEX A**SECTION 1 -- SECURITY (CONT'D)****YES****NO**

- | | | |
|-------|-------|---|
| _____ | _____ | 27. Is all COMSEC material properly stored when not being used and under the direct control of authorized personnel? [CMS 21A, Article 520.a(2)] |
| <hr/> | | |
| _____ | _____ | 28. Are COMSEC files, records and logs conspicuously marked and stored in accordance with the highest overall classification of the contents? [CMS 21A, Article 715.a; SECNAVINST 5510.36, Article 6-3, 6-26] |
| <hr/> | | |
| _____ | _____ | 29. Are classified COMSEC files, records and logs annotated with the following statement?
[CMS 21A, Article, 715.d(2)(c)]

"Derived from: CMS 21A
Declassify on: X1" |
| <hr/> | | |

SECTION 2 -- EKMS MANAGER RESPONSIBILITIES

- | | | |
|-------|-------|--|
| _____ | _____ | 30. Are the alternate manager(s) kept fully informed of the status of the command account so they are at all times fully capable of assuming the EKMS Manager's duties? [CMS 21A, Article 455.d] |
| <hr/> | | |
| _____ | _____ | 31. Does the EKMS Manager provide the CO/OIC, SCMSRO and other interested personnel with general information about new or revised CMS policies or procedures? [CMS 21A, Article 455.a] |
| <hr/> | | |

ANNEX A

SECTION 2 -- EKMS MANAGER RESPONSIBILITIES (CONT'D).

YES	NO	
_____	_____	32. Has the EKMS Manager promulgated written guidance and/or publication extracts concerning the proper handling, accountability, and disposition of COMSEC material, including STU-III terminals and key, to all Local Element (LE) personnel? [CMS 21A, Article 455.e, 721 NOTE, 769.a, CMS 6, Article 240.a(5)]
<hr/>		
_____	_____	33. Has the EKMS Manager promulgated guidance to the LEs concerning specific files (reports, messages, correspondence) they are required to maintain? [CMS 21A, Article 703 NOTE 2]
<hr/>		
_____	_____	34. Has the EKMS Manager promulgated instructions/guidance to (Issuing) LE's on the proper maintenance of their Accountable Item (A/I) Summary? [CMS 21A, Article 763.d]
<hr/>		
_____	_____	35. Have all military LE personnel (except USMC/USCG) completed the CMS User Personnel Qualification Standards (PQS) (NAVEDTRA 43462 series)? [CMS 21A, Article 450.f]
<hr/>		
_____	_____	36. Does the EKMS Manager conduct training with all personnel handling COMSEC material to ensure they are adhering to proper EKMS procedures? [CMS 21A, Article 455.f]
<hr/>		

ANNEX A

SECTION 2 -- EKMS MANAGER RESPONSIBILITIES (CONT'D)

YES	NO	
_____	_____	37. Has the EKMS Manager ensured that all training is properly documented in accordance with command directives? [CMS 21A, Article 455.f; OPNAVINST 3120.32B, Article 811]
<hr/>		
_____	_____	38. Does the EKMS Manager conduct periodic spot checks on LE(s)? [CMS 21A, Article 455.k]
<hr/>		
_____	_____	39. Are "COMSEC Responsibility Acknowledgement Forms" completed and handled as follows: [CMS 21A, Article 769.b(2); Annex K]
_____	_____	a. Properly completed for each individual that handles COMSEC material and filed in the Chronological File?
<hr/>		
_____	_____	b. Retained for 90 days after the individual no longer requires access to CMS material?
<hr/>		
_____	_____	40. Has the EKMS Manager ensured the provisions of OPNAVINST 2221.5 are met prior to releasing COMSEC material to a contractor? [CMS 21A, Article 505.g]
<hr/>		
_____	_____	41. If the account has LEs which are responsible to a CO other than the account EKMS Manager's CO, has the EKMS Manager ensured that Letters of Agreement were exchanged? [CMS 21A, Article 445, Annex L]
<hr/>		

ANNEX A

SECTION 2 -- EKMS MANAGER RESPONSIBILITIES (CONT'D)

YES	NO	
_____	_____	42. Does the Letter of Agreement address the minimum issues in accordance with CMS 21A? [CMS 21A, Annex L] _____
_____	_____	43. Is a copy of the completed, Letter of Agreement held by the EKMS Manager in the Directives File? [CMS 21A, Article 709.c] _____
_____	_____	44. Has coordination been made with the area Defense Courier Service (DCS) station to establish a DCS account by submission of a DCS Form 10? [CMS 21A, Article 405.h(1)] _____
_____	_____	45. Does the EKMS Manager ensure that all cryptographic maintenance personnel that perform maintenance within his/her account, have DD 1435(s) documented and on file? [OPNAVINST 2221.3 (series); CMS 5A, Article 150.b] _____
_____	_____	46. Has a formal designation Letter or Memorandum of Appointment (LOA/MOA) been completed for the EKMS Manager and Alternate(s)? [CMS 21A, Article 425.a; Annex J] _____
_____	_____	47. Does the EKMS Manager and Alternate(s) meet the minimum designation requirements specified in CMS 21A? [CMS 21A, Article 415] _____

ANNEX A

SECTION 2 -- EKMS MANAGER RESPONSIBILITIES (CONT'D)

YES

NO

- _____ 48. Is the LOA/MOA signed by the CO and retained for a minimum of two years following the relief of the EKMS Manager? [CMS 21A, Article 425.b; Annex J Note (1)]
- _____ 49. Does the EKMS Manager ensure modifications to COMSEC equipment are maintained currently by checking against MMVG and CMS 5A? [CMS 21A, Article 455.t, 757.g; CMS 5A, Article 350]

Section 3 -- ACCOUNT CLERK

- _____ 50. Have all military Account Clerks (except USMC/USCG) completed the CMS Clerk PQS (NAVEDTRA 43462 series)? [CMS 21A, Article 450.f]
- _____ 51. Has a formal designation Letter or Memorandum of Appointment (LOA/MOA) been completed for the Account Clerk? [CMS 21A, Article 420.e]
- _____ 52. Is the Account Clerk restricted from having access to combinations to the COMSEC material vault/safe/security containers, and only allowed to maintain TPI requirements after the COMSEC container has been opened by Manager personnel? [CMS 21A, Article 470.a(2)]

ANNEX A

SECTION 3 -- ACCOUNT CLERK (CONT'D)

YES

NO

_____ 53. Are all receipts, inventories, and destruction reports that are signed by the clerk, signed as a witness only? [CMS 21A, Article 470.a(4)]

SECTION 4 -- LCMS/NEAT/CARS

_____ 54. Are the LMD monitor, KP, and STU-III arranged to allow the operator to view all displays without obstruction? [CMS 21A, Annex AA, paragraph 10.b]

_____ 55. Is LCMS being used to maintain records for all COMSEC material held by the account? [CMS 21A, Article 718.b]

_____ 56. Does the account maintain a KP CIK ID log? [CMS 21A, Annex AA, paragraph 10.a]

_____ 57. Are PINs for the KP CIK's changed every 6 months? [CMS 21A, Article 520.j(4); Annex AA, paragraph 10.a]

_____ 58. Are PIN's/Passwords for all LMD/KP Administrators and Operators recorded and sealed in an SF-700 envelope and protected as specified in CMS 21A? [CMS 21A, Article 520.j; Annex AA, paragraph 7 NOTE]

ANNEX A

SECTION 4 -- LCMS/NEAT/CARS (CONT'D)

YES	NO	
_____	_____	59. Do all EKMS Managers/Alternate personnel have their own unique LCMS/KP Operator ID's? [CMS 21A, Annex AA, paragraph 10.a] _____
_____	_____	60. Does the account have two LMD/KP System Administrators registered? [CMS 21A, Article 150.a, Annex AA, paragraph 7] _____
_____	_____	61. Has the account performed a changeover every 3 months to update the encryption key used by the KP? [CMS 21A, Annex AA, paragraph 10.u] _____
_____	_____	62. Has the account performed a KP rekey on an annual basis? [CMS 21A, Annex AA, paragraph 10.v] _____
_____	_____	63. Has the KP been re-certified in the last 3 years? [CMS 21A, Article 1185.d] _____
_____	_____	64. Has the account archived LCMS data at least every 6 months? [CMS 21A, Annex AA, paragraph 10.t] _____
_____	_____	65. Are the KP REINIT1 and REINIT2 keys appropriately classified and safeguarded? [CMS 21A, Article 520.j(1)] _____

ANNEX A

SECTION 4 -- LCMS/NEAT/CARS (CONT'D)

YES

NO

- _____ 66. Are backups being performed periodically as required? [CMS 21A, Article 718.d]
- NOTE:** Required backups are LCMS Database, SCO Unix "ROOT" and "/u/usr"
-
- _____ 67. Is magnetic media (tapes, floppy diskettes) used for backups classified "SECRET" and clearly labeled with the date the backup was performed? [CMS 21A, Article 718.c NOTE]
-
- _____ 68. Are files that have been transferred to DCMS retained until a subsequent DCMS-generated SF-153 Inventory is received that indicates the transaction was processed correctly? [CMS 21A, Annex F, paragraph 10.a]
-

SECTION 5 -- CHRONOLOGICAL FILE

69. Does the CHRONOLOGICAL FILE contain the following required files:
[CMS 21A, Article 706.a]
- _____ a. COMSEC material accounting reports (i.e., receipts, transfers, destruction, generation, possession and relief of accountability)
- _____ b. Accountable Item (A/I) Summary, if printed copy maintained
- _____ c. Inventory reports (i.e. COR generated SF-153, working copies).
- _____ d. Transaction Status Log, if printed copy maintained

ANNEX A**SECTION 5 -- CHRONOLOGICAL FILE (CONT'D)****YES****NO**

- | | | |
|-------|-------|---|
| _____ | _____ | e. DCS Form 10 and CMS Form 1 (if required) |
| _____ | _____ | f. COMSEC Responsibility Acknowledgement Form |
-

SECTION 6 -- TRANSACTION STATUS LOG

- | | | |
|-------|-------|--|
| _____ | _____ | 70. Is the Transaction Status Log on file in the chronological file up-to-date? [CMS 21A, Article 718.b(2); Annex T paragraph 2.s] |
|-------|-------|--|

NOTE: Printouts are optional if records are maintained electronically.

- | | | |
|-------|-------|--|
| _____ | _____ | 71. Is a copy retained in the chronological file at the end of each calendar year and is it annotated on the bottom of the last page certifying the last TN of that calendar year? [CMS 21A, Annex U, paragraph 4] |
|-------|-------|--|
-

SECTION 7 -- COMSEC MATERIAL RECEIPTS/TRANSFERS

- | | | |
|-------|-------|---|
| _____ | _____ | 72. Are SF-153 COMSEC material Receipt Reports for physical material properly completed to include: TN number, date assigned, type of action, EKMS Manager/Alternate and witness signatures (witness is only required for TPI material)? [CMS 21A, Annex V] |
|-------|-------|---|
-

ANNEX A

SECTION 7 -- COMSEC MATERIAL RECEIPTS/TRANSFERS
(CONT'D)

YES	NO	
_____	_____	73. Do inter-service SF-153 transfer reports originated by DON EKMS accounts (e.g., a transfer between a DON account and other service account such as USA, USAF) contain the required transfer statement? [CMS 21A, Article 733.a(2) Note]
_____	_____	74. Have ETRs been sent to DCMS for physical material SF-153 Receipt and Transfer Reports using CARS or GENSER messages? [CMS 21A, Article 742.a(1)(a)] NOTE: During periods of EMCON or MINIMIZE the completed SF-153 should be appropriately annotated and forwarded via mail to DCMS. [CMS 21A, Article 742.b(3) and Annex W, paragraph 2.b]
_____	_____	75. Are ETRs transmitted via GENSER message addressed to DCMS WASHINGTON DC//30// and a copy attached to the corresponding SF-153 report? [CMS 21A, Annex W, paragraph 9.e and Annex W, Tab 1, paragraph 4.b(2)]
_____	_____	76. Has the EKMS Manager ensured that an ETR Receipt report has been forwarded within 96 hours after receiving physical COMSEC material? [CMS 21A, Article 742.b(1); Annex W, Tab 1, paragraph 2.b]

ANNEX A

SECTION 7 -- COMSEC MATERIAL RECEIPTS/TRANSFERS
(CONT'D)

YES

NO

- _____ 77. Are transaction ETRs that are reported to DCMS via CARS annotated with "transmitted via CARS on YYMMDD", attached to the printed SF-153 and filed in the chronological file? [CMS 21A, Annex W, Tab 1, paragraph 4.a(2)]
-
- _____ 78. Has the receipt of Two Person Control (TPC) material been reported per CJCSI 3260.01? [CMS 21A, Article 255.d; Annex W, Article 9.g(2), Tab 1,; paragraph 3.b and 8.e NOTE]
-
- _____ 79. Are discrepancies noted in the receipt process reported IAW guidance outlined in CMS 21A? [CMS 21A, Article 742.c and 754]
-

SECTION 8 -- DESTRUCTION PROCEDURES/REPORTS

- _____ 80. Is routine destruction of COMSEC material performed IAW the methods prescribed in CMS 21A? [CMS 21A, Article 790]
-
- _____ 81. Are destruction records being completed to document the destruction of all Top Secret and Secret COMSEC material and all ALC 1 and 2 COMSEC material regardless of its classification? [CMS 21A, Article 736.b(2)]
-

ANNEX A

SECTION 8 -- DESTRUCTION PROCEDURES/REPORTS
(CONT'D)

YES	NO	
_____	_____	82. Is destruction of key maintained or issued in a DTD being completed in accordance with CMS 21A? [CMS 21A, Annex AC, paragraph 15 and Article 540.c(3)(a)]
_____	_____	83. Do destruction records clearly identify the short title, edition(s), accounting number, ALC, and date of destruction? [CMS 21A, Article 736.a(3); Figures 7-1, 7-2, 7-3; Annex V]
_____	_____	84. Are LE destruction records properly signed, or initialed, by the two individuals who conducted the destruction? [CMS 21A, Article 790.f(1)(2); Figures 7-1, 7-2, 7-3; Annex V]
_____	_____	85. Is unissued keying material that becomes superseded during the month destroyed no later than five working days after the end of the month in which it was superseded? [CMS 21A, Article 540.e and 540.f(3)(a)]
_____	_____	86. Is superseded material received in a ROB shipment destroyed within 12 hours of opening the shipment and the SF-153 destruction document annotated "superseded on receipt?" [CMS 21A, Article 540.e(8)]

ANNEX A

SECTION 8 -- DESTRUCTION PROCEDURES/REPORTS
(CONT'D)

YES

NO

- _____ 87. Does the account end-of-month consolidated destruction reports that are filed in the Chronological File consist of both the Reportable and Local Destruction Reports (vice working copies)? [CMS 21A, Article 706.a(1) and 736.b]
-
- _____ 88. Have consolidated destruction records been signed by the Commanding Officer? [CMS 21A, Annex V, paragraph 7.a]
-
- _____ 89. Are SAS/TPC destruction reports signed by two members of the SAS/TPC team? [CMS 21A, Annex V, paragraph 7.b]
-

SECTION 9 -- DCMS-GENERATED FIXED CYCLE (FC)
INVENTORY REPORTS

- _____ 90. Is the first CY FC inventory completed and returned to DCMS no later than 60 days from the "prepared by" date for all ALC 1,2,4,6 and 7 keying material, publications, manuals and equipment? [CMS 21A, Article 766.a(1)(2); 766.b(1)(c); Annex Z paragraph 4.a]
-

ANNEX A

SECTION 9 -- DCMS-GENERATED FIXED CYCLE (FC)
INVENTORY REPORTS (CONT'D)

YES	NO	
_____	_____	91. Has the DCMS-generated procedural check-off list been updated during the first CY FC/Combined inventory to reflect the type of inventory conducted and the current account status (e.g., date of last CMS A&A visit; COMSEC inspection; PLA/ISIC verification)? [CMS 21A, Annex Z, paragraph 3]
_____	_____	92. If ALC 4 or 7 material is held by the account, was a locally generated inventory listing all ALC 4 or 7 material used in conjunction with the DCMS-generated SF-153 to complete and document the FC inventories? [CMS 21A, Article 766.e(3)]
_____	_____	93. Is the <u>second</u> CY FC inventory completed for all ALC 1,2,4,6 and 7 key holdings? [CMS 21A, Article 766.a(1), 766.b(1)(e)]
_____	_____	94. Are completed FC inventories signed by the EKMS Manager and/or Alternate who conducted the inventory, a qualified witness, and the CO, OIC or SCMSRO? [CMS 21A, Annex Z, paragraph 9; Annex V paragraph 7]
_____	_____	95. Are FC and Combined inventories completed only through the preprinted TN on the procedural check-off list? [CMS 21A, Annex Z, paragraph 4.a]

ANNEX A

**SECTION 9 -- DCMS-GENERATED FIXED CYCLE (FC)
INVENTORY REPORTS (CONT'D)****YES****NO**

_____ 96. Are file copies and working copies of Fixed Cycle, Combined, Special inventories retained in accordance with CMS 21A? [CMS 21A, Annex T, paragraph 2.j]

**SECTION 10 -- COMBINED/SPECIAL DCMS-GENERATED
INVENTORY REPORTS**

_____ 97. If a Combined or Special inventory was conducted due to a Change of Command, was the inventory signed by the outgoing Commanding Officer? [CMS 21A, Article 766.a(3)(a)]

_____ 98. If a Combined or Special inventory was conducted due to a Change of EKMS MANAGER, was the inventory conducted by the outgoing EKMS Manager and witnessed by the incoming EKMS Manager? [CMS 21A, Article 766.g(1)(a)]

_____ 99. If a Special inventory was conducted, was the pre-printed TN and date on the procedural check-off list adjusted to reflect the most current TN? [CMS 21A, Annex Z, paragraph 5.a]

ANNEX A

SECTION 11 -- COMPLETING SF-153 INVENTORY REPORTS

YES	NO	
_____	_____	100. Are line-outs, additions and/or adjustment entries on the original SF-153 inventory report properly annotated? [CMS 21A, Annex Z, paragraph 7] _____
		101. If a Fixed-Cycle or Combined Inventory was conducted and material was added, has the following been complied with: [CMS 21A, Annex Z, paragraph 8]
_____	_____	a. Has additional ALC-1, ALC-2 and ALC-6 material which was received prior to the pre-printed TN of the inventory been added to a separate SF-153? _____
_____	_____	b. Are the words " <u>Add-On Sheet</u> " inserted in the "TO" block of the SF-153? _____
_____	_____	c. Is all material listed on the add-on sheet in the same format as the listings on the inventory (i.e., alphanumeric order), and each entry single-spaced? _____
_____	_____	d. Does the first beginning line number on the add-on sheet follow in sequential order from the last line number of the inventory? _____
_____	_____	e. For each line item listed on the add-on page, is the item's associated receipt TN annotated in the remark's column? _____

ANNEX A

SECTION 11 -- COMPLETING SF-153 INVENTORY REPORTS
(CONT'D)

YES

NO

_____ _____ f. Have the total number of lines and total number of items added to the Add-On Sheet been annotated on the SF-153?

_____ _____ 102. Were required copies of EKMS accounting reports appended to the inventory for each reportable TN annotated on the COR-generated SF-153s that were received prior to the pre-printed TN? [CMS 21A, Annex Z, paragraph 10.b]

SECTION 12 -- CORRESPONDENCE, MESSAGE AND DIRECTIVES
FILE

103. Does the CMS Correspondence and Message File contain the following required files:
[CMS 21A, Article 709]

_____ _____ a. EKMS account establishment correspondence?

NOTE: Mandatory for accounts established after 01 Jul 93; optional for previously established accounts.

_____ _____ b. EKMS Manager and Clerk appointment correspondence?

_____ _____ c. Primary LE (Issuing) and Alternate(s) appointment correspondence and LH CBT completion certificate?

ANNEX A

SECTION 12 -- CORRESPONDENCE, MESSAGE AND DIRECTIVES
FILE (CONT'D)

YES	NO	
_____	_____	d. COMSEC incident and PDS reports? _____
_____	_____	e. Correspondence relating to command allowance and authorization to store classified COMSEC material? _____
_____	_____	f. CMS Updates/EKMS Newsletters? _____
_____	_____	g. CMS Assist Visit and Inspection correspondence? <u>NOTE:</u> CMS A&A Visits are optional for Navy EKMS accounts. _____
_____	_____	h. List of personnel authorized access to keying material and the LMD/KP? _____
_____	_____	104. Does the directives file contain a copy of the Letter of Agreement and each effective command and higher authority directive which relates to CMS matters? [CMS 21A, Article 709.c] _____

ANNEX A

SECTION 13 -- COMSEC LIBRARY

YES

NO

_____ 105. Does the account maintain a COMSEC library with all applicable instructions/manuals? [CMS 21A, Article 721]

SECTION 14 -- GENERAL MESSAGE FILE (GMF)

_____ 106. Is a GMF maintained and does it contain a copy of all effective, general messages (i.e., ALCOMs, ALCOMPAC, ALCOMLANT) that relate to COMSEC matters? [CMS 21A, Article 709.b]

NOTE: Review ALCOM 01/"current year" for effective ALCOMs of the previous year.

SECTION 15 -- LOCAL CUSTODY FILE

_____ 107. Does the local custody file contain signed, effective, local custody documents for each item of COMSEC material charged to the account which has been issued to authorized LEs? [CMS 21A, Article 712]

_____ 108. Are local custody documents being retained for the minimum 90 days after supersession? [CMS 21A, Annex T, paragraph 2.b]

ANNEX A

SECTION 16 -- REPORT RETENTION/DISPOSITION

YES	NO	
_____	_____	109. Are inactive records awaiting expiration of the required retention period clearly labeled with the appropriate classification and the authorized destruction date? [CMS 21A, Article 715.c] _____
		110. Have the following been retained for the <u>minimum</u> retention period of one year: [CMS 21A, Annex T]
_____	_____	a. Receipts for official messenger mail, courier mail and registered mail? _____
_____	_____	b. Administrative and receipt records pertaining to DCS? _____
		111. Have the following been retained for the <u>minimum</u> retention period of two years: [CMS 21A, Annex T]
_____	_____	a. Destruction records (i.e., SF-153) for SECRET and above material? _____
_____	_____	b. General correspondence and messages relating to account holdings? _____
_____	_____	c. Transaction Status Logs (if maintained manually and at a minimum the End of Year closeout record)? _____

ANNEX A

SECTION 16 -- REPORT RETENTION/DISPOSITION (CONT'D)

YES

NO

_____ _____ d. Fixed Cycle/Combined inventories (including
Local Element inventory report(s))?

SECTION 17 -- RESEALING/STATUS MARKINGS

_____ _____ 112. Were the procedures for sealing/resealing
COMSEC material accomplished in accordance
with CMS 21A and local command
instruction(s)? [CMS 21A, Article 772]

_____ _____ 113. Does the EKMS Manager maintain effective/
supersession dates for all COMSEC material
held by the account? [CMS 21A, Article
760.a; Annex AB paragraph 5.c]

_____ _____ 114. Does the EKMS Manager maintain the account
C2MSR? [CMS 21A, Article 255.a]

_____ _____ 115. For accounts with less than 500 line items,
are the effective and supersession dates
annotated on all physical COMSEC keying
material, COMSEC accountable manuals and
publications? [CMS 21A, Article 760.a]

NOTE: This requirement applies to watch
station material, as well.

ANNEX A

SECTION 17 -- RESEALING/STATUS MARKINGS (CONT'D)

YES

NO

_____ 116. Are keytape canisters free of locally applied labels and stickers which may conceal attempted penetration or prevent inspection of protective packaging? [CMS 21A, Article 760.e and 760.f]

_____ 117. For accounts with 500 or more line items, are the effective and supersession dates for physical material annotated in LCMS in the Effective Date Tool upon receipt and on material prior to issue to Local Element personnel? [CMS 21A, Article 760.a]

SECTION 18 -- PAGECHECKS

_____ 118. Are required page/verification checks being accomplished as follows:
[CMS 21A, Articles 757, 775.e, and Annex Y]

_____ a. Unsealed COMSEC keying material: upon initial receipt; during account and watch inventories; upon transfer; and upon destruction?

_____ b. Unsealed maintenance and operating manuals: upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during Fixed-Cycle (Equip/Pubs) and Change of EKMS Manager inventories; upon transfer; and upon destruction?

ANNEX A

SECTION 18 -- PAGECHECKS (CONT'D)

YES	NO	
_____	_____	c. <u>Unsealed amendments</u> : upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during Fixed-Cycle (Equip/Pubs) and Change of EKMS Manager inventories; during watch inventories; upon transfer; and upon destruction? _____
_____	_____	d. <u>Maintenance and repair kits</u> : All components upon initial receipt; transfer; and upon destruction. Classified components only upon installation of modification; during Fixed-Cycle (Equip/Pubs) and change of EKMS Manager inventories? _____
_____	_____	e. <u>Equipment</u> : upon receipt (i.e., uncrating); during Fixed-Cycle (Equip/Pubs) and change of EKMS Manager inventories; during watch inventories; upon transfer; and upon destruction? _____
_____	_____	f. <u>Resealed keying material</u> : during account inventories; upon transfer; and upon destruction? _____
_____	_____	119. Are pagecheck discrepancies being reported? [CMS 21A, Article 757.h; Annex X] _____

ANNEX A

SECTION 19 -- CORRECTIONS AND AMENDMENTS

YES	NO	
_____	_____	120. Are corrections to a publication made with black or blue-black ink only? [CMS 21A, Article 787.g(1)(b)(1)]
<hr/>		
_____	_____	121. Are pen and ink corrections identified by writing the amendment or correction number in the margin opposite the correction? [CMS 21A, Article 787.g(1)(b)(2)]
<hr/>		
_____	_____	122. Has the person entering the amendment signed and dated the appropriate blanks on the publication's Record of Amendments page? [CMS 21A, Article 787.g(2)(a)]
<hr/>		
_____	_____	123. Has the individual who verified proper entry of the amendment initialed the entry on the Record of Amendments page? [CMS 21A, Article 787.g(5)(b)]
<hr/>		
_____	_____	124. If pages were removed, substituted, or added; have both the person entering the amendment and the person verifying the amendment conducted a pagecheck of the publication and recorded this on the Record of Pagecheck page? [CMS 21A, Article 787.g(4), and 787.g(5)(c)]
<hr/>		

ANNEX A

SECTION 19 -- CORRECTIONS AND AMENDMENTS (CONT'D)

YES

NO

_____ 125. Does the EKMS Manager ensure that amendment residue is destroyed within five working days of amendment entry? [CMS 21A, Article 787.h(2) NOTE]

SECTION 20 -- STU-III

_____ 126. Are STU-III terminals being accounted for within LCMS? [CMS 6, Article 205]

_____ 127. Does the account maintain a Running Inventory (R/I) for STU-III keying material which is accountable to the EKMS Central Facility (CF)? [CMS 6, Article 530]

_____ 128. Does the EKMS account Chronological File contain the following STU-III files:
[CMS 6, Article 505.a]

_____ a. Record copies of Key Conversion Notices (KCNs)?

_____ b. EKMS CF STU-III Keying Material TN Log?
[CMS 6, Article 525]

_____ c. EKMS CF SF-153 accounting reports (i.e. receipts, transfers, destruction, possession, relief of accountability)

ANNEX A

SECTION 20 -- STU III (CONT'D)

YES	NO	
_____	_____	d. EKMS CF STU-III Keying material Semi-annual Inventory Reports. _____
_____	_____	129. Does the EKMS account Correspondence, Message and Directives file contain a copy of each effective command and higher authority directive which relates to STU-III matters? [CMS 6, Article 510.a] _____
_____	_____	130. Does the EKMS account Local Custody file contain signed, effective local custody documents for issued STU-III keying material and terminals? [CMS 6, Article 240.a(6), 301.e(2), 515.a] _____
_____	_____	131. Does the EKMS account maintain a CIK Data Log which contains the minimum information in accordance with CMS 6 to locally account for STU-III Master and User CIKs?: [CMS 6, Article 535.a; Annex F] _____
_____	_____	132. If Master CIKs retained, are they stored in a GSA approved security container by the account EKMS Manager or a Master Control User only? [CMS 6, Article 250.b(3), 250.c(3)] _____
_____	_____	133. Has the account received and completed an EKMS CF semi-annual STU-III key inventory? [CMS 6, Article 701.a(2), 701.b] _____

ANNEX A

SECTION 20 -- STU III (CONT'D)

YES

NO

- _____ 134. Are original destruction records forwarded to the EKMS CF and a copy retained locally in accordance with CMS 6 for the following: [CMS 6, Article 415]
- a. When an unused FD is loaded into a terminal for the express purpose of zeroizing it?
- b. When operational key is loaded into a terminal?
- c. When Seed key is loaded into a terminal and the conversion call cannot be made or is unsuccessful?
-

SECTION 21 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR TRANSFER (OTAT)

NOTE: If a Key Variable Generator (KVG) (i.e., KG-83, KGX-93/93A) is not held in the account, skip to question 139.

- _____ 135. Has the KVG(s) been certified by an authorized facility prior to initial use, every two years thereafter, if security control was lost for any reason and after maintenance/repair? [CMS 21A, Article 1145.b and 1145.c]
-
- _____ 136. Have NSA-furnished tamper detection labels been applied to certified/ recertified KVG(s)? [CMS 21A, Article 1145.h]
-

ANNEX A

**SECTION 21 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR
TRANSFER (OTAT) (CONT'D)****YES****NO**

- | | | |
|--|-------|--|
| <hr/> | <hr/> | 137. Does each certified KVG have a certification tag on a handle that displays the classification of the equipment, "CRYPTO" status, date of certification, command that performed certification, and name/rank of the certifying technician? [CMS 21A, Article 1145.i] |
| <hr/> | | |
| <hr/> | <hr/> | 138. Have fill devices containing electronic key been clearly labeled (tagged/marked) with the identity of the key it contains? [CMS 21A, Article 1175.b(2)] |
| <hr/> | | |
| <hr/> | <hr/> | 139. If the account generates, transmits, relays or receives electronic key, are local accounting records being maintained? [CMS 21A, Article 1175.b(2) and 1182.d] |
| <p>NOTE: Recipients of key received via OTAR are not required to maintain accounting records.</p> | | |
| <hr/> | | |
| <hr/> | <hr/> | 140. If the account generates electronic key for OTAR and/or OTAT, have accounting records been retained for a minimum of 60 days following the date of the last entry on the key generation log? [CMS 21A, Article 1182.d(1)] |
| <hr/> | | |

ANNEX A

**SECTION 21 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR
TRANSFER (OTAT) (CONT'D)****YES****NO**

_____ 141. If the account relays or receives electronic key (except for receipt of key via OTAR), are local accounting records being retained until the key is superseded? [CMS 21A, Article 1182.d(2)]

_____ 142. Does the EKMS Manager (or Alternate) conduct a periodic review of OTAT/OTAR local accounting logs? [CMS 21A, Article 455.j; 1115.c]

SECTION 22 -- DATA TRANSFER DEVICE (DTD)

_____ 143. Is a classification tag attached to the DTD via the lanyard ring to indicate handling requirements when the Crypto Ignition Key (CIK) is not inserted? [CMS 21A, Annex AC, paragraph 8.f]

_____ 144. Is a tag attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number? [CMS 21A, Annex AC, paragraph 9.c]

ANNEX A

SECTION 22 -- DATA TRANSFER DEVICE (DTD) (CONT'D)

YES

NO

_____ 145. For accounts with a Top Secret CIK, is the CIK removed from the DTD and returned to TPI storage when authorized Users are not present? [CMS 21A, Annex AC, paragraph 10.b]

NOTE: Otherwise, both CIK and DTD must be continually safeguarded according to TPI rules.

_____ 146. Is unrestricted access to Supervisory CIKs limited to only those individuals who are authorized to perform all of the associated privileges? [CMS 21A, Annex AC, paragraph 11.d]

_____ 147. Does the account ensure that key is not stored on the DTD host side? [CMS 21A, Annex AC, paragraph 12.b]

NOTE: Any known violations of this rule must be reported in accordance with CMS 21A, Chapter 9.

_____ 148. Have recipients of key issued in a DTD, from any source other than a LMD/KP, signed a local custody document acknowledging receipt of the key? [CMS 21A, Annex AC, paragraph 13.c]

ANNEX A

SECTION 22 -- DATA TRANSFER DEVICE (DTD) (CONT'D)

YES

NO

_____ 149. Does the EKMS Manager or Supervisory User locally account for all DTD CIKs by assigned serial number? [CMS 21A, Annex AC, paragraph 7.b]

_____ 150. For **non-watch station** environments, are the Supervisory and User CIKs inventoried whenever the account conducts Fixed-Cycle or Combined inventories? [CMS 21A, Annex AC, paragraph 14.a(1)]

_____ 151. For **watch station** environments, are the serial numbers of Supervisory CIKs, User CIKs, and DTDs visually verified whenever watch personnel change? [CMS 21A, Annex AC, paragraph 14.b(1)]

NOTE: The watch-to-watch inventory will serve as the record of inventory.

_____ 152. Is the DTD audit trail data reviewed by appropriate personnel at least once per month and these reviews recorded in an Audit Review Log? [CMS 21A, Article 540.c(3)(a) Annex AC, paragraph 17.b, 17.c and 17.d]

_____ 153. Is the Audit Review Log retained at least two years? [CMS 21A, Annex AC, paragraph 17.f(2)]

ANNEX A

SECTION 23 -- EMERGENCY PROTECTION OF COMSEC MATERIAL

YES	NO	
_____	_____	154. Has the command prepared an Emergency Action Plan (EAP) for safeguarding COMSEC material, including STU-III terminals, keys and CIKs, in the event of an emergency? [CMS 21A, Annex M, paragraph 2.a; SECNAVINST 5510.36, exhibit 2B; CMS 6, Article 860]
<hr/>		
_____	_____	155. Are all authorized personnel at the facility made aware of the existence of the EAP? [CMS 21A, Annex M, paragraph 6.d(2)]
<hr/>		
_____	_____	156. For commands, located within the continental United States (CONUS), does the EAP provide guidance detailing actions to be taken for natural disasters, civil/mob actions and terrorism? [CMS 21A, Annex M, paragraph 2.b]
<hr/>		
_____	_____	157. For commands located outside CONUS, does the EAP provide detailed guidance for both natural disasters and hostile actions? [CMS 21A, Annex M, paragraph 2.c]
<hr/>		
		158. Have plans been incorporated into the command's EAP to accomplish the following actions during natural disasters: [CMS 21A, Annex M, paragraph 4]
_____	_____	a. Fire reporting and initial fire fighting by assigned personnel?
<hr/>		

ANNEX A

SECTION 23 -- EMERGENCY PROTECTION OF COMSEC
MATERIAL (CONT'D)

YES	NO	
_____	_____	b. Assignment of on-the-scene responsibility for protecting COMSEC material held? _____
_____	_____	c. Protecting material when admitting outside fire fighters into the secure area(s)? _____
_____	_____	d. Securing or removing classified COMSEC material and evacuating the area(s)? _____
_____	_____	e. Assessing and reporting probable exposure of classified COMSEC material to unauthorized persons during the emergency? _____
_____	_____	f. Completing a post-emergency inventory of COMSEC and Controlled Cryptographic Item (CCI) material and reporting any losses or unauthorized exposures to appropriate authorities? _____
_____	_____	159. Are EAP training exercises conducted annually to ensure that everyone is familiar with their assigned duties? [CMS 21A, Annex M, paragraph 6.d(3)] _____

ANNEX A

SECTION 24 -- EMERGENCY DESTRUCTION PLAN (EDP)

YES

NO

NOTE: The questions in this section apply only to EKMS accounts and/or their Local Elements that are located outside CONUS or are onboard a mobile platform that deploys outside CONUS.

- _____ 160. Does the EKMS account have an EDP incorporated into their EAP? [CMS 21A, Annex M, paragraph 2.g, 2.j and 2.k]
-
- _____ 161. Does the EDP identify personnel assignments and the chain of authority that is authorized to make the determination that emergency destruction is to begin? [CMS 21A, Annex M, paragraph 5.d(5) and 5.d(6); SECNAVINST 5510.36, Exhibit 2B PART II paragraph 4]
-
- _____ 162. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [CMS 21A, Annex M, paragraph 5.d, 6.c]
-
- _____ 163. Are the sensitive pages of KAMs prepared for **ready** removal (i.e., upper left corner clipped) and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [CMS 21A, Annex M, paragraph 5.e(2)(a)]
-
- _____ 164. Are the priorities of destruction indicated in the plan? [CMS 21A, Annex M, paragraph 8]
-

ANNEX A

SECTION 24 -- EMERGENCY DESTRUCTION PLAN (EDP)
(CONT'D)

- | YES | NO | |
|-------|-------|---|
| _____ | _____ | 165. Are EDP training exercises conducted on an annual basis to ensure that everyone is familiar with their duties? [CMS 21A, Annex M, paragraph 6.d(3)] |
| <hr/> | | |
| _____ | _____ | 166. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [CMS 21A, Annex M, paragraph 7] |
| <hr/> | | |
| _____ | _____ | 167. Does the EDP provide for adequate identification and rapid reporting of the material destroyed, to include the method and extent of destruction?
[CMS 21A, Annex M, paragraph 10] |
| <hr/> | | |
| _____ | _____ | 168. Does the EDP stress that accurate information concerning the extent of emergency destruction is second in importance only to the destruction of the material itself?
[CMS 21A, Annex M, paragraph 10.a] |
| <hr/> | | |
| _____ | _____ | 169. Are document sinking bags available in sufficient quantity and in good condition to permit jettison of COMSEC material?
(NOTE: Surface units only)
[CMS 21A, Annex M, paragraph 9.d(2)(b)] |
| <hr/> | | |

ANNEX A

**SECTION 25 -- COMMANDING OFFICER (CO, OIC, SCMSRO)
RESPONSIBILITIES**

YES NO

170. Has the CO ensured the following:

_____ _____ a. All COMSEC incidents and PDS(s) are promptly reported and action taken, as required?
[CMS 21A, Article 450.e, 930.a, Annex D, paragraph 3]

_____ _____ b. Unannounced spot checks for EKMS Managers and spaces where COMSEC material is used and stored are conducted at least quarterly?
[CMS 21A, Article 450.h, Annex D, paragraph 5]

SECTION 26 -- MATERIAL ACCOUNTABILITY TRACKING

171. Randomly select three COMSEC short titles from an incoming SF-153 and trace the items throughout the command EKMS account to ensure material is properly handled. (EKMS 704 LMD/KP Operator's Manual, pages 4-5 through 4-8 and pages 8-22 through 8-36)

NOTE: To check random short titles, perform the following steps in LCMS:

STEPS

1. From the LCMS desktop menu, select **ACCOUNTING --> INVENTORY --> ACCOUNTABLE ITEMS SUMMARY.**
2. The Element Selection window appears and shows the EKMS ID/Element Name for the local account and all registered Local Elements. To review the current accountable items for the local account:
 - a. Click on (highlight) the **account EKMS ID/Element Name.**
 - b. Click on the **SELECT** button.

ANNEX A

SECTION 26 -- MATERIAL ACCOUNTABILITY TRACKING
(CONT'D)

3. To view detailed data for one of the selected short titles:

NOTE: If the desired short title is not listed, skip to step number 6.

- a. click on (highlight) the **short title** entry.
- b. click on the **Detailed Data** button.
- c. the Detailed Data window provides the following:
 - 1) identifies the material as **On-Hand or Issued**.
 - 2) the EKMS ID/Element Name of the **element accountable** for the item.
 - 3) **short title identification information**.

4. To review the associated history of transactions for an item listed on the Detailed Data window:

- a. click on (highlight) desired entry and click on the **Material History** button.
- b. The Material Item History window appears and provides a listing of **all Accounting Transactions** in which the selected material is referenced.

5. **Skip to step number 10 and answer associated questions.**

6. If the desired short title was not located during step 3, perform the following: (EKMS 704, Pages 8-22 through 8-26)

- a. From the LCMS desktop menu, select **UTILITY --> QUERY TOOL --> ADD**.
- b. From the Query window, make the following selections:
 - 1) Query Type: **ACCOUNTING REPORTS**.
 - 2) Results Format: **LONG**.
 - 3) Query Action: **EXECUTE**.
 - 4) Query Name: **type in a name** (i.e. Inspect1).
 - 5) click the **PROCESS** button.

ANNEX A

**SECTION 26 -- MATERIAL ACCOUNTABILITY TRACKING
(CONT'D)**

c. From the Accounting Reports window, perform the following:

- 1) select: **NATIONAL SHORT TITLE.**
- 2) enter the desired **SHORT TITLE.**
- 3) press: **ENTER Key.**
- 4) select: **EDITION.**
- 5) enter the desired short title edition.
- 6) press: **ENTER Key.**
- 7) select: **PROCESS.**
- 8) exit back to the LCMS Main Menu.

d. Double-click on the Query Results icon with the associated name given in step 6.b.4 above.

NOTE: If information on the desired short title is not listed, skip to step number 8.

7. Skip to step number 10 and answer associated questions.

8. If the desired short title was not located during step 6, perform the following: (EKMS 704 pages 8-32 through 8-36)

- a. Reload Archive Data. From the LCMS desktop menu, select **UTILITY -->ARCHIVE --> RETRIEVE DATA.**
- b. Load the Archive Tape or Disk in the appropriate drive.
- c. On the Load Media window, make the following selections:
 - 1) Media Type: **TAPE or DISK** as appropriate.
 - 2) UNIX Device Name: for **tape** **/dev/rStp0**
for **disk** **/dev/rfd0135ds18**
 - 3) Click the **RETRIEVE** button.
 - 4) Ensure media is loaded and click **CONTINUE** on the Archive Advisory window.
 - 5) Click **RETRIEVE** on the Media Identification window.
 - 6) Upon completion of the Retrieve, click **EXIT.**

ANNEX A

**SECTION 26 -- MATERIAL ACCOUNTABILITY TRACKING
(CONT'D)**

- d. From the LCMS desktop menu, select **UTILITY --> ARCHIVE --> QUERY RETRIEVED DATA --> ADD.**
- e. From the Query window, make the following selections:
- 1) Query Type: **ACCOUNTING REPORTS.**
 - 2) Results Format: **LONG.**
 - 3) Query Action: **EXECUTE.**
 - 4) Query Name: **type in a name** (i.e. Inspect1).
 - 5) click the **PROCESS** button.
- f. From the Accounting Reports window, perform the following:
- 1) select: **NATIONAL SHORT TITLE.**
 - 2) enter the desired **SHORT TITLE.**
 - 3) press: **ENTER Key.**
 - 4) select: **EDITION.**
 - 5) enter the desired short title edition.
 - 6) press: **ENTER Key.**
 - 7) select: **PROCESS.**
 - 8) exit back to the LCMS Main Menu.
- g. Double-click on the Query Results icon with the associated name given in step 8.e.4 above.

NOTE: If information on the desired short title is not listed, reload the next Archive Data Tape or Disk and repeat step number 8.

9. Skip to step number 10 and answer associated questions.

10. Answer the following questions:

YES NO

a. **Material listed as "On-Hand":**

_____ Does the account have a record of receipt?

ANNEX A

SECTION 26 -- MATERIAL ACCOUNTABILITY TRACKING
(CONT'D)

_____ Does the account have a record of an ETR being
sent to DCMS?

_____ Is the material stored in the account COMSEC
vault?

b. **Material listed as "Issued":**

_____ Does the account have a record of receipt?

_____ Does the account have a record of an ETR being
sent to DCMS?

_____ Does the account have a record of Local
Custody Issue?

_____ Is the material stored by the Local Element
listed?

c. **Material which has already been "Destroyed":**

_____ Does the account have a record of receipt?

_____ Does account have a record of an ETR being
sent to DCMS?

ANNEX A

SECTION 26 -- MATERIAL ACCOUNTABILITY TRACKING
(CONT'D)

_____ _____ Was material destroyed within the required
time frame?

_____ _____ Does the account have the consolidated
destruction report signed by the Commanding
Officer?

COMMENTS:

<p align="center"> ANNEX B EKMS INSPECTION GUIDE LOCAL ELEMENT (ISSUING) </p>
--

PURPOSE. The purpose of this inspection guide is to ensure all aspects of COMSEC management are covered by the EKMS inspectors during the account inspection.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

Immediate Superior in Command (if other than EKMS Inspector)
of Unit Inspected: _____

Date of Last Inspection: _____

Name/Grade/Rate and Command of EKMS Inspector:

Date of Last Facilities Approval: _____

Primary Local Element (Issuing) Name/Grade:

Alternate Local Element (Issuing) Name/Grade:

Identify Following, as Applicable/Assigned:

Second Alternate Local Element (Issuing) Name/Grade:

Third Alternate Local Element (Issuing) Name/Grade:

Account Clerk Name/Grade: _____

ANNEX B
EKMS INSPECTION GUIDE
LOCAL ELEMENT (ISSUING)

SECTION IDENTIFICATION

- 1 - Security
- 2 - Local Element (Issuing) Responsibilities
- 3 - Account Clerk
- 4 - Accountable Items (A/I) Summary
- 5 - Local Custody File
- 6 - Resealing/Status Markings
- 7 - Pagechecks
- 8 - Corrections and Amendments
- 9 - Destruction Procedures/Reports
- 10 - Over-the-Air-Rekey (OTAR)/Over-the-Air-Transfer
 (OTAT)
- 11 - Data Transfer Device (DTD)
- 12 - Emergency Protection of COMSEC Material
- 13 - Emergency Destruction Plan (EDP)

<p align="center">ANNEX B</p> <p align="center">EKMS INSPECTION GUIDE</p> <p align="center">LOCAL ELEMENT (ISSUING)</p>
--

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the EKMS Inspector conducting the inspection. Per Chapter 2 and Article 401.c., inspection reports evaluated as unsatisfactory must include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to annotate comments to any question that receives a negative response. This inclusion in the inspection checklists should greatly aid inspectors and commands when conducting the out-brief and writing the official report of inspection results.

SECTION 1 -- SECURITY

NOTE: Inspect COMSEC vault using Annex D or E as appropriate

YES	NO	
_____	_____	<p>1. Are adequate visitor controls enforced to ensure that access to classified information is given only to visitors who possess the proper identification, security clearance, and NEED TO KNOW? [SECNAVINST 5510.30A, Article 11-1 paragraph 2,3; SECNAVINST 5510.36, Article 7-11; CMS 21A, Article 550.e]</p> <p>_____</p>
_____	_____	<p>2. Is a visitor's register maintained and retained for one year from the date the register was completed? [CMS 21A, Article 550.e; Annex T]</p> <p>_____</p>
_____	_____	<p>3. Is unescorted access limited to individuals whose duties require such access and who meet access requirements? [CMS 21A, Articles 505, 535, 550.e]</p> <p>_____</p>

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	4. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list? [CMS 21A, Article 550.e]
<hr/>		
_____	_____	5. <u>PART A:</u> Are personnel whose duties require access to COMSEC material formally authorized in writing by the CO? [CMS 21A, Article 450.c and 505.d]
<hr/>		
_____	_____	<u>PART B:</u> If personnel are authorized access to COMSEC material on an access list, has the list been updated annually or whenever the status of an individual changed? [CMS 21A, Article 505.d(2)]
<hr/>		
_____	_____	6. Do all personnel having access to COMSEC material have a clearance equal to or greater than the highest classification of the material? [CMS 21A, Article 505.a]
<hr/>		
_____	_____	7. Is security clearance data of personnel whose duties require access to COMSEC material maintained by the Command Security Manager? [SECNAVINST 5510.30A, Article 9-5 paragraphs 2,3,4,5]
 <u>NOTE:</u> For Marine Corps, documented in the Marine Corps Total Force System (MCTFS). For Coast Guard, documented in the Personnel Management Information System (PMIS).		
<hr/>		

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

- | YES | NO | |
|-------|-------|--|
| _____ | _____ | 8. Has formal facility approval been given in writing, by ISIC or higher authority, to hold classified COMSEC material? [CMS 21A, Article 405.a(2), 405.g(2) and 550.d(1)] |
| <hr/> | | |
| _____ | _____ | 9. Is the exterior of each COMSEC security container free of markings which reveal the classification of the material stored therein? [SECNAVINST 5510.36, Article 10-1, paragraph 3] |
| <hr/> | | |
| _____ | _____ | 10. Is the space/compartment or vault which contains COMSEC material outwardly identified as "RESTRICTED AREA"? [OPNAVINST 5530.14C, Article 0319.d, Appendixes VI, VII] |
| <hr/> | | |
| _____ | _____ | 11. Are applicable security controls (e.g., guards and alarms) in place in accordance with SECNAVINST 5510.36, Chapter 10? [CMS 21A, Article 520.a(3)] |
| <hr/> | | |
| _____ | _____ | 12. Do storage containers meet the minimum security requirements for the highest classification of keying material stored therein? [CMS 21A, Article 520.c, 520.d and 520.e; SECNAVINST 5510.36, Chapter 10] |

NOTE: Effective 14 April 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any classified material. [CMS 21A, Article 520.f]

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	13. Is a Maintenance Record for Security Containers and Vault Doors (Optional Form 89) maintained for each security container and retained within the container? [SECNAVINST 5510.36, Article 10-15, paragraph 3, Exhibit 10C; CMS 21A, Article 520.b(3)]
_____	_____	14. Are all damages, repairs or alterations to the container or parts of the container (e.g., Group 1R locks, locking drawer, drawer head, etc.) properly documented on an Optional Form 89? [SECNAVINST 5510.36, Article 10-15, paragraph 3; CMS 21A, Article 520.b(3)]
_____	_____	15. Do storage containers conform to the two-person integrity (TPI) requirements for the protection of Top Secret COMSEC keying material? [CMS 21A, Article 520.e]
_____	_____	16. Is a Security Container Information Form (SF 700) maintained for each lock combination and placed in each COMSEC security container? [SECNAVINST 5510.36, Article 10-12, paragraph 3; CMS 21A, Article 520.b(1)]
_____	_____	17. Is a Security Container Check Sheet (SF-702) maintained for each lock combination of a COMSEC storage container? [SECNAVINST 5510.36, Article 7-10; CMS 21A, Article 520.b(2)]

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	<p>18. Except in an emergency, are combinations to the COMSEC Account vault/security containers restricted to the Primary (Issuing) Local Element (LE) and Alternates only? [CMS 21A, Article 515.c(1)]</p> <hr/>
_____	_____	<p>19. If the COMSEC facility is continuously manned, are security checks conducted at least once every 24 hours? [CMS 21A, Article 550.d(3)(a)]</p> <p>NOTE: Recorded in accordance with local command directives (e.g., line item on watch-to-watch inventory or SF-701).</p> <hr/>
_____	_____	<p>20. In a non-continuously manned COMSEC facility, are security checks conducted prior to departure of the last person and documented using the Activity Security Checklist (SF-701)? [CMS 21A, Article 550.d(3)(b); SECNAVINST 5510.36, Article 7-10]</p> <hr/>
_____	_____	<p>21. If a COMSEC facility is in a high risk area and unmanned for periods greater than 24 hours, is a check conducted at least once every 24 hours to ensure that all doors are locked and that there have been no attempts at forceful entry. [CMS 21A, Article 550.d(3)(c)]</p> <p>NOTE: Recorded in accordance with local command directives (e.g., annotated on SF-702).</p> <hr/>

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

YES

NO

_____ 22. Does any one person have knowledge of both combinations to any one TPI container? [CMS 21A, Article 515.c(2)]

NOTE: A "Yes" answer on this question constitutes non-compliance. A "No" answer on this question constitutes compliance.

_____ 23. Are all sealed records of combinations to COMSEC containers maintained in an approved security container (other than the container where the COMSEC material is stored), and available to duty personnel for emergency use? [CMS 21A, Article 515.e]

_____ 24. Are combinations to COMSEC containers changed when initially placed in use, taken out of service, upon transfer/reassignment of personnel who have access, or when compromised? [SECNAVINST 5510.36, Article 10-12; CMS 21A, Article 515.b]

_____ 25. Is each COMSEC security container record of combination protected as follows: [CMS 21A, Article 515.f]

_____ a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope?

_____ b. Combination envelope sealed using transparent lamination or plastic tape?

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	c. Name(s) and address(es) of individual(s) authorized access to the combination recorded on the front of the envelope? _____
_____	_____	d. Proper classification markings on envelope? [CMS 21A, Article 515.d] _____
_____	_____	e. Are the envelopes inspected monthly to ensure they have not been tampered with? _____
_____	_____	26. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and segregated by status, type and classification? (Example: Effective, Secret keymat <u>not</u> stored with superseded, Secret keymat or effective, Top Secret keymat <u>not</u> stored with effective, Confidential keymat.) [CMS 21A, Article 520.a(4); Annex M, paragraph 3.b] _____
_____	_____	27. When not being used and under the direct control of authorized personnel, is all COMSEC material properly stored? [CMS 21A, Article 520.a(2)] _____

ANNEX B

SECTION 1 -- SECURITY (CONT'D)

YES

NO

_____ 28. Are COMSEC files, records and logs conspicuously marked and stored in accordance with the highest overall classification of the contents? [CMS 21A, Article 715.a; SECNAVINST 5510.36, Article 6-3, 6-26]

_____ 29. Are classified COMSEC files, records and logs annotated with the following statement? [CMS 21A, Article 715.d(2)(c)]

"Derived from: CMS 21A
Declassify on: X1"

SECTION 2 -- LOCAL ELEMENT (ISSUING)
RESPONSIBILITIES

_____ 30. Are the alternate manager(s) kept fully informed of the status of the command account so they are at all times fully capable of assuming the Primary (Issuing) LE's duties? [CMS 21A, Article 460.b]

_____ 31. Does the Primary (Issuing) LE provide the CO/OIC, SCMSRO and other interested personnel with general information about new or revised CMS policies or procedures? [CMS 21A, Article 465.a]

ANNEX B

SECTION 2 -- LOCAL ELEMENT (ISSUING)
RESPONSIBILITIES (CONT'D)

YES	NO	
_____	_____	<p>32. Does the (Issuing) LE hold the written guidance and/or publication extracts (provided by the parent account EKMS Manager) concerning the proper handling, accountability, and disposition of COMSEC material, including STU-III terminals and key? [CMS 21A, Article 465.b]</p> <p>_____</p>
_____	_____	<p>33. Has the (Issuing) LE promulgated written guidance and/or publication extracts concerning the proper handling, accountability, and disposition of COMSEC material, including STU-III terminals and key, to all Local Element (LE) personnel? [CMS 21A, Article 465.c]</p> <p>_____</p>
_____	_____	<p>34. Have all military LE personnel (except USMC/USCG) completed the CMS User Personnel Qualification Standards (PQS) (NAVEDTRA 43462 series)? [CMS 21A, Article 450.f]</p> <p>_____</p>
_____	_____	<p>35. Does the (Issuing) LE conduct training with all personnel handling COMSEC material to ensure they are adhering to proper EKMS procedures? [CMS 21A, Article 465.c]</p> <p>_____</p>
_____	_____	<p>36. Has the (Issuing) LE ensured that all training is properly documented in accordance with command directives? [CMS 21A, Article 465.c; OPNAVINST 3120.32B, Article 811]</p> <p>_____</p>

ANNEX B

SECTION 2 -- LOCAL ELEMENT (ISSUING)
RESPONSIBILITIES (CONT'D)

YES**NO**

37. Are "COMSEC Responsibility Acknowledgement Forms" completed and handled as follows:
 [CMS 21A, Article 769.b(2); Annex K]

_____ _____ a. Properly completed for each individual
 that handles COMSEC material and filed in
 the Chronological File?

_____ _____ b. Retained for 90 days after the individual
 no longer requires access to CMS material?

_____ _____ 38. If the (Issuing) LE has LEs which are
 responsible to a CO other than the Primary
 (Issuing) LE's CO, has the Primary (Issuing)
 LE ensured that Letters of Agreement were
 exchanged? [CMS 21A, Article 445, Annex L]

_____ _____ 39. Does the Letter of Agreement address the
 minimum issues in accordance with CMS 21A?
 [CMS 21A, Annex L]

_____ _____ 40. Is a copy of the completed, Letter of
 Agreement held by the Primary (Issuing) LE?
 [CMS 21A, Article 709.c]

ANNEX B

SECTION 2 -- LOCAL ELEMENT (ISSUING)
RESPONSIBILITIES (CONT'D)

YES	NO	
_____	_____	<p>41. Does the Primary (Issuing) LE ensure that all cryptographic maintenance personnel that perform maintenance within his/her account, have DD 1435(s) documented and on file? [OPNAVINST 2221.3 (series); CMS 5A, Article 150.b]</p> <p>_____</p>
_____	_____	<p>42. Has a formal designation Letter or Memorandum of Appointment (LOA/MOA) been completed and signed by the CO for the Primary (Issuing) LE and Alternate(s)? [CMS 21A, Article 425.a; Annex J]</p> <p>_____</p>
_____	_____	<p>43. Does the Primary (Issuing) LE and Alternate(s) meet the minimum designation requirements specified in CMS 21A? [CMS 21A, Article 420]</p> <p>_____</p>
_____	_____	<p>44. Has the LOA/MOA and LH CBT Certificate of Completion been forwarded to the parent account EKMS Manager and a copy retained on file for a minimum of two years following the relief of the Primary (Issuing) LE and/or Alternate(s)? [CMS 21A, Article 425.b; Annex J Note (1)]</p> <p>_____</p>
_____	_____	<p>45. Does the (Issuing) LE maintain required files as directed by the parent account EKMS Manager? [CMS 21A, Article 703 NOTE 2]</p> <p>_____</p>

ANNEX B**SECTION 3 -- ACCOUNT CLERK****YES****NO**

- | | | |
|-------|-------|--|
| <hr/> | <hr/> | 46. Have all military Account Clerks (except USMC/USCG) completed the CMS Clerk PQS (NAVEDTRA 43462 series)? [CMS 21A, Article 450.f] |
| <hr/> | | |
| <hr/> | <hr/> | 47. Has a formal designation Letter or Memorandum of Appointment (LOA/MOA) been completed for the Account Clerk? [CMS 21A, Article 420.e] |
| <hr/> | | |
| <hr/> | <hr/> | 48. Is the Account Clerk restricted from having access to combinations to the COMSEC material vault/safe/security containers, and only allowed to maintain TPI requirements after the COMSEC container has been opened by Manager personnel? [CMS 21A, Article 470.a(2)] |
| <hr/> | | |
| <hr/> | <hr/> | 49. Are all receipts, inventories, and destruction reports that are signed by the clerk, signed as a <u>witness</u> only? [CMS 21A, Article 470.a(4)] |
| <hr/> | | |

SECTION 4 -- ACCOUNTABLE ITEMS (A/I) SUMMARY

- | | | |
|-------|-------|---|
| <hr/> | <hr/> | 50. Does the (Issuing) LE maintain an Accountable Item (A/I) Summary as instructed by the parent account EKMS Manager? [CMS 21A, Article 763.d] |
| <hr/> | | |

ANNEX B

SECTION 5 -- LOCAL CUSTODY FILE

YES

NO

- _____ 51. Does the local custody file contain signed, effective, local custody documents for each item of COMSEC material charged to the (Issuing) LE which has been issued to authorized LEs? [CMS 21A, Article 712]
-
- _____ 52. Do the local custody documents (i.e., SF 153, or locally prepared equivalent), contain the minimum required information? [CMS 21A, Article 769.c(1)]
-
- _____ 53. Are local custody documents being retained for the minimum 90 days after supersession? [CMS 21A, Annex T, paragraph 2.b]
-

SECTION 6 -- RESEALING/STATUS MARKINGS

- _____ 54. Were the procedures for sealing/resealing COMSEC material accomplished in accordance with CMS 21A and local command instruction(s)? [CMS 21A, Article 772]
-
- _____ 55. Are the effective and supersession dates annotated on all COMSEC keying material, COMSEC accountable manuals and publications in accordance with CMS 21A? [CMS 21A, Article 760.a, 775.g]
-

ANNEX B

SECTION 6 -- RESEALING/STATUS MARKINGS (CONT'D)

YES

NO

_____ 56. Are keytape canisters free of locally applied labels and stickers which may conceal attempted penetration or prevent inspection of protective packaging? [CMS 21A, Article 760.e and 760.f]

SECTION 7 -- PAGECHECKS

_____ 57. Are required page/verification checks being accomplished as follows:
[CMS 21A, Articles 757, 775.e, and Annex Y]

_____ a. Unsealed COMSEC keying material: upon initial receipt; during account and watch inventories; upon transfer; and upon destruction?

_____ b. Unsealed maintenance and operating manuals: upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during Fixed-Cycle (Equip/Pubs) and Change of EKMS Manager inventories; upon transfer; and upon destruction?

_____ c. Unsealed amendments: upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during Fixed-Cycle (Equip/Pubs) and Change of EKMS Manager inventories; during watch inventories; upon transfer; and upon destruction?

ANNEX B

SECTION 7 -- PAGECHECKS (CONT'D)

YES	NO	
_____	_____	d. <u>Maintenance and repair kits</u> : All components upon initial receipt; transfer; and upon destruction. Classified components only upon installation of modification; during Fixed-Cycle (Equip/Pubs) and change of EKMS Manager inventories?
_____	_____	e. <u>Equipment</u> : upon receipt (i.e., uncrating); during Fixed-Cycle (Equip/Pubs) and change of EKMS Manager inventories; during watch inventories; upon transfer; and upon destruction?
_____	_____	f. <u>Resealed keying material</u> : during account inventories; upon transfer; and upon destruction?
_____	_____	58. Are pagecheck discrepancies being reported? [CMS 21A, Article 757.h; Annex X]

SECTION 8 -- CORRECTIONS AND AMENDMENTS

_____	_____	59. Are amendments to COMSEC publications current and properly entered? [CMS 21A, Article 787]
_____	_____	60. Are corrections to a publication made with black or blue-black ink only? [CMS 21A, Article 787.g(1)(b)(1)]

ANNEX B

SECTION 8 -- CORRECTIONS AND AMENDMENTS (CONT'D)

YES

NO

- | | | | |
|-------|-------|-----|---|
| _____ | _____ | 61. | Are pen and ink corrections identified by writing the amendment or correction number in the margin opposite the correction? [CMS 21A, Article 787.g(1)(b)(2)] |
| <hr/> | | | |
| _____ | _____ | 62. | Has the person entering the amendment signed and dated the appropriate blanks on the publication's Record of Amendments page? [CMS 21A, Article 787.g(2)(a)] |
| <hr/> | | | |
| _____ | _____ | 63. | Has the individual who verified proper entry of the amendment initialed the entry on the Record of Amendments page? [CMS 21A, Article 787.g(5)(b)] |
| <hr/> | | | |
| _____ | _____ | 64. | If pages were removed, substituted, or added; have both the person entering the amendment and the person verifying the amendment conducted a pagecheck of the publication and recorded this on the Record of Pagecheck page? [CMS 21A, Article 787.g(4), and 787.g(5)(c)] |
| <hr/> | | | |

SECTION 9 -- DESTRUCTION PROCEDURES/REPORTS

- | | | | |
|-------|-------|-----|--|
| _____ | _____ | 65. | Are local destruction records being completed to document the destruction of all Top Secret and Secret COMSEC material and all ALC 1 and 2 COMSEC material regardless of its classification? [CMS 21A, Article 736.b(2)] |
| <hr/> | | | |

ANNEX B

SECTION 9 -- DESTRUCTION PROCEDURES/REPORTS
(CONT'D)

YES	NO	
_____	_____	66. Do destruction records clearly identify the short title, edition(s), accounting number, ALC, and date of destruction? [CMS 21A, Article 736.a(3); Figures 7-1, 7-2, 7-3; Annex V] _____
_____	_____	67. Are LE destruction records properly signed, or initialed, by the two individuals who conducted the destruction? [CMS 21A, Article 790.f(1)(2); Figures 7-1, 7-2, 7-3; Annex V] _____
_____	_____	68. Do local destruction records for segmented COMSEC material contain the following: [CMS 21A, Chapter 7 Fig 7-1, 7-2, 7-3]
_____	_____	a. Short title and complete accounting data? _____
_____	_____	b. Date of destruction? _____
_____	_____	c. Signatures of the two individuals conducting destruction? _____
_____	_____	d. Classification/Declassification markings? Derived from: CMS 21A Declassify on: X1 _____
_____	_____	e. Marked "CONFIDENTIAL (When filled in)"? _____

ANNEX B

SECTION 9 -- DESTRUCTION PROCEDURES/REPORTS
(CONT'D)

YES	NO	
_____	_____	69. Is <u>only</u> one copy of a short title, edition, and accounting number recorded on the CMS 25 or locally prepared segmented destruction document? [CMS 21A, Figure 7-1, paragraph 8]
_____	_____	70. Is routine destruction of COMSEC material performed IAW the methods prescribed in CMS 21A? [CMS 21A, Article 790]
_____	_____	71. Is destruction of key maintained or issued in a DTD being completed in accordance with CMS 21A? [CMS 21A, Annex AC, paragraph 15 and Article 540.c(3)(a)]
_____	_____	72. Is unissued keying material that becomes superseded during the month destroyed no later than five working days after the end of the month in which it was superseded? [CMS 21A, Article 540.e and 540.f(3)(a)]
_____	_____	73. Can Local Element personnel demonstrate the proper procedures for conducting routine destruction of COMSEC material? [CMS 21A, Article 540 and 790]

ANNEX B

SECTION 9 -- DESTRUCTION PROCEDURES/REPORTS
(CONT'D)

YES NO

74. If keying material was unintentionally removed from its protective canister, is the following documentation recorded on its associated disposition record:
 [CMS 21A, Article 772.d]

_____ _____ a. A statement that the keytape segment(s) were unintentionally removed?

_____ _____ b. The date of the unintentional removal?

_____ _____ c. Identity of the keytape segment(s) actually removed?

_____ _____ d. Signatures of the individuals who removed the key?

SECTION 10 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR
TRANSFER (OTAT)

NOTE: If a Key Variable Generator (KVG) (i.e., KG-83, KGX-93/93A) is not held in the account, skip to question 79.

_____ _____ 75. Has the KVG(s) been certified by an authorized facility prior to initial use, every two years thereafter, if security control was lost for any reason and after maintenance/repair? [CMS 21A, Article 1145.b and 1145.c]

ANNEX B

SECTION 10 -- OVER-THE-AIR-REKEY (OTAR)/ OVER-THE-AIR-TRANSFER (OTAT) (CONT'D)

YES	NO	
_____	_____	76. Have NSA-furnished tamper detection labels been applied to certified/ recertified KVG(s)? [CMS 21A, Article 1145.h]
<hr/>		
_____	_____	77. Does each certified KVG have a certification tag on a handle that displays the classification of the equipment, "CRYPTO" status, date of certification, command that performed certification, and name/rank of the certifying technician? [CMS 21A, Article 1145.i]
<hr/>		
_____	_____	78. Have fill devices containing electronic key been clearly labeled (tagged/marked) with the identity of the key it contains? [CMS 21A, Article 1175.b(2)]
<hr/>		
_____	_____	79. If the LE generates, transmits, relays or receives electronic key, are local accounting records being maintained? [CMS 21A, Article 1175.b(2) and 1182.d]
<p>NOTE: Recipients of key received via OTAR are not required to maintain accounting records.</p>		
<hr/>		
_____	_____	80. If the LE generates electronic key for OTAR and/or OTAT, have accounting records been retained for a minimum of 60 days following the date of the last entry on the key generation log? [CMS 21A, Article 1182.d(1)]
<hr/>		

ANNEX B

**SECTION 10 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR
TRANSFER (OTAT) (CONT'D)**

YES

NO

_____ 81. If the LE relays or receives electronic key (except for receipt of key via OTAR), are local accounting records being retained until the key is superseded? [CMS 21A, Article 1182.d(2)]

_____ 82. Does the Primary (Issuing) LE (or Alternate) conduct a periodic review of OTAT/OTAR local accounting logs? [CMS 21A, Article 465.i and 1115.c]

SECTION 11 -- DATA TRANSFER DEVICE (DTD)

_____ 83. Is a classification tag attached to the DTD via the lanyard ring to indicate handling requirements when the Crypto Ignition Key (CIK) is not inserted? [CMS 21A, Annex AC, paragraph 8.f]

_____ 84. Is a tag attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number? [CMS 21A, Annex AC, paragraph 9.c]

_____ 85. For accounts with a Top Secret CIK, is the CIK removed from the DTD and returned to TPI storage when authorized Users are not present? [CMS 21A, Annex AC, paragraph 10.b]

NOTE: Otherwise, both CIK and DTD must be continually safeguarded according to TPI rules.

ANNEX B

SECTION 11 -- DATA TRANSFER DEVICE (DTD) (CONT'D)

YES	NO	
_____	_____	86. Is unrestricted access to Supervisory CIKs limited to only those individuals who are authorized to perform all of the associated privileges? [CMS 21A, Annex AC, paragraph 11.d] _____
_____	_____	87. Does the account ensure that key is <u>not</u> stored on the DTD host side? [CMS 21A, Annex AC, paragraph 12.b] NOTE: Any known violations of this rule must be reported in accordance with CMS 21A, Chapter 9. _____
_____	_____	88. Have recipients of key issued in a DTD, from any source other than a LMD/KP, signed a local custody document acknowledging receipt of the key? [CMS 21A, Annex AC, paragraph 13.c] _____
_____	_____	89. Does the (Issuing) LE or Supervisory User locally account for all DTD CIKs by assigned serial number? [CMS 21A, Annex AC, paragraph 7.b] _____
_____	_____	90. For non-watch station environments, are the Supervisory and User CIKs inventoried whenever the parent account conducts Fixed-Cycle or Combined inventories? [CMS 21A, Annex AC, paragraph 14.a(1)] _____

ANNEX B

SECTION 11 -- DATA TRANSFER DEVICE (DTD) (CONT'D)

YES

NO

_____ 91. For **watch station** environments, are the serial numbers of Supervisory CIKs, User CIKs, and DTDs visually verified whenever watch personnel change? [CMS 21A, Annex AC, paragraph 14.b(1)]

NOTE: The watch-to-watch inventory will serve as the record of inventory.

_____ 92. Is the DTD audit trail data reviewed by appropriate personnel at least once per month and these reviews recorded in an Audit Review Log? [CMS 21A, Article 540.c(3)(a) Annex AC, paragraph 17.b, 17.c and 17.d]

_____ 93. Is the Audit Review Log retained at least two years? [CMS 21A, Annex AC, paragraph 17.f(2)]

SECTION 12 -- EMERGENCY PROTECTION OF COMSEC MATERIAL

_____ 94. Has the command prepared an Emergency Action Plan (EAP) for safeguarding COMSEC material, including STU-III terminals, keys and CIKs, in the event of an emergency? [CMS 21A, Annex M, paragraph 2.a; SECNAVINST 5510.36, exhibit 2B; CMS 6, Article 860]

_____ 95. Are all authorized personnel at the facility made aware of the existence of the EAP? [CMS 21A, Annex M, paragraph 6.d(2)]

ANNEX B

SECTION 12 -- EMERGENCY PROTECTION OF COMSEC
MATERIAL (CONT'D)

YES	NO	
_____	_____	96. For commands, located within the continental United States (CONUS), does the EAP provide guidance detailing actions to be taken for natural disasters, civil/mob actions and terrorism? [CMS 21A, Annex M, paragraph 2.b] _____
_____	_____	97. For commands located outside CONUS, does the EAP provide detailed guidance for both natural disasters and hostile actions? [CMS 21A, Annex M, paragraph 2.c] _____
_____	_____	98. Have plans been incorporated into the command's EAP to accomplish the following actions during natural disasters: [CMS 21A, Annex M, paragraph 4]
_____	_____	a. Fire reporting and initial fire fighting by assigned personnel? _____
_____	_____	b. Assignment of on-the-scene responsibility for protecting COMSEC material held? _____
_____	_____	c. Protecting material when admitting outside fire fighters into the secure area(s)? _____
_____	_____	d. Securing or removing classified COMSEC material and evacuating the area(s)? _____

ANNEX B

SECTION 12 -- EMERGENCY PROTECTION OF COMSEC
MATERIAL (CONT'D)

- | YES | NO | |
|-------|-------|--|
| _____ | _____ | e. Assessing and reporting probable exposure of classified COMSEC material to unauthorized persons during the emergency? |
| <hr/> | | |
| _____ | _____ | f. Completing a post-emergency inventory of COMSEC and Controlled Cryptographic Item (CCI) material and reporting any losses or unauthorized exposures to appropriate authorities? |
| <hr/> | | |
| _____ | _____ | 99. Are EAP training exercises conducted annually to ensure that everyone is familiar with their assigned duties? [CMS 21A, Annex M, paragraph 6.d(3)] |
| <hr/> | | |

SECTION 13 -- EMERGENCY DESTRUCTION PLAN (EDP)

NOTE: The questions in this section apply only to EKMS accounts and/or their Local Elements that are located outside CONUS or are onboard a mobile platform that deploys outside CONUS.

- | | | |
|-------|-------|--|
| _____ | _____ | 100. Does the (Issuing) Local Element have an EDP incorporated into their EAP? [CMS 21A, Article 465.1; Annex M, paragraph 2.g, 2.j and 2.k] |
| <hr/> | | |

ANNEX B

SECTION 13 -- EMERGENCY DESTRUCTION PLAN (EDP)
(CONT'D)

YES	NO	
_____	_____	101. Does the EDP identify personnel assignments and the chain of authority that is authorized to make the determination that emergency destruction is to begin? [CMS 21A, Annex M, paragraph 5.d(5) and 5.d(6); SECNAVINST 5510.36, Exhibit 2B PART II paragraph 4] _____
_____	_____	102. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [CMS 21A, Annex M, paragraph 5.d, 6.c] _____
_____	_____	103. Are the sensitive pages of KAMs prepared for ready removal (i.e., upper left corner clipped) and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [CMS 21A, Annex M, paragraph 5.e(2)(a)] _____
_____	_____	104. Are the priorities of destruction indicated in the plan? [CMS 21A, Annex M, paragraph 8] _____
_____	_____	105. Are EDP training exercises conducted on an annual basis to ensure that everyone is familiar with their duties? [CMS 21A, Annex M, paragraph 6.d(3)] _____
_____	_____	106. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [CMS 21A, Annex M, paragraph 7] _____

ANNEX B

SECTION 13 -- EMERGENCY DESTRUCTION PLAN (EDP)
(CONT'D)

YES

NO

- | | | |
|-------|-------|---|
| _____ | _____ | 107. Does the EDP provide for adequate identification and rapid reporting of the material destroyed, to include the method and extent of destruction?
[CMS 21A, Annex M, paragraph 10] |
| <hr/> | | |
| _____ | _____ | 108. Does the EDP stress that accurate information concerning the extent of emergency destruction is second in importance only to the destruction of the material itself?
[CMS 21A, Annex M, paragraph 10.a] |
| <hr/> | | |
| _____ | _____ | 109. Are document sinking bags available in sufficient quantity and in good condition to permit jettison of COMSEC material?
(<u>NOTE</u> : Surface units only)
[CMS 21A, Annex M, paragraph 9.d(2)(b)] |
| <hr/> | | |

ANNEX C
INSPECTION GUIDE
LOCAL ELEMENT -
USING

PURPOSE. The purpose of this inspection guide is to ensure all aspects of COMSEC management are covered by the EKMS Inspectors during the account inspection.

INITIAL REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

Immediate Superior in Command (if other than EKMS Inspector) of
Unit Inspected: _____

Date of Last Inspection: _____

Name/Grade/Rate and Command of Inspector: _____

Date of Last Facilities Approval: _____

EKMS Manager Name/Grade: _____

Primary Alternate EKMS Manager Name/Grade: _____

Identify Following, as Applicable/Assigned:

Second Alternate EKMS Manager Name/Grade: _____

Third Alternate EKMS Manager Name/Grade: _____

<p style="text-align: center;">ANNEX C INSPECTION GUIDE LOCAL ELEMENT - USING</p>
--

SECTION IDENTIFICATION

- 1 - Security
- 2 - Local Element (Using) Responsibilities
- 3 - Local Custody File
- 4 - Watch Station Inventory/Pagechecks
- 5 - Resealing/Status Markings
- 6 - Corrections and Amendments
- 7 - Routine Destruction
- 8 - Data Transfer Device (DTD)
- 9 - Over-the-Air-Rekey/Over-the-Air-Transfer (OTAR/OTAT)
- 10 - Emergency Action Plan (EAP)
- 11 - Emergency Destruction Plan (EDP)

<p style="text-align: center;">ANNEX C INSPECTION GUIDE LOCAL ELEMENT - USING</p>
--

ACTION. The following inspection checklist shall be used and completed, in its entirety, by the Inspector conducting the inspection. Per Chapter 2 and Article 401.c., inspection reports evaluated as unsatisfactory must include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to annotate comments to any question that receives a negative response. This inclusion in the inspection checklists should greatly aid inspectors and commands when conducting the out-brief and writing the official report of inspection results.

SECTION 1 -- SECURITY

NOTE: Inspect COMSEC facility using Annex D or E as appropriate.

- | YES | NO | |
|-------|-------|--|
| _____ | _____ | 1. If <u>not</u> continuously manned, is the main entrance to the COMSEC facility equipped with a GSA-approved, electro-mechanical lock meeting Federal Specification FF-L-2740? [CMS 21A, Annex O, paragraph 4.b(2)] |
| <hr/> | | |
| _____ | _____ | 2. If continuously manned, is the main entrance to the COMSEC facility designed to accommodate a combination electro-mechanical lock meeting Federal Specification FF-L-2740 and a dead bolt should it be necessary to evacuate the facility? [CMS 21A, Annex O, paragraph 4.b(2)] |

NOTE: Facilities equipped with a GSA-approved built-in Group-1R lock prior to 01 Apr 93 may continue to use the Group-1 lock.

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	3. Is the entrance to the COMSEC facility arranged so that persons seeking entry can be identified without being admitted to the spaces or being able to view classified material? [CMS 21A, Annex O, paragraph 4.b(4)]
_____	_____	4. Is the COMSEC Facility outwardly identified only as a "RESTRICTED AREA"? [OPNAVINST 5530.14C, Article 0319.d, Appendix VI, VII]
_____	_____	5. Are windows secured in a permanent manner to prevent them from being opened and screened to prevent inadvertent viewing of the space's interior from an exterior point? (The protection provided to the windows need be no stronger than the strength of the contiguous walls.) [CMS 21A, Annex O, paragraph 5]
_____	_____	6. Is only one door used for regular entrance to the facility? [CMS 21A, Annex O, paragraph 4]
_____	_____	7. Are emergency exits designed so that they can be opened only from inside the COMSEC facility? [CMS 21A, Annex O, paragraph 4.b(3)]

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	8. Are all air vents, ducts or any similar openings which breach the walls, floor or ceiling appropriately secured to prevent penetration? [CMS 21A, Annex O, paragraph 6] _____
_____	_____	9. Are applicable security controls (e.g., guards, alarms) in place in accordance with SECNAVINST 5510.36, Chapter 10? [CMS 21A, Article 520.a.(3)] _____
_____	_____	10. Are personally owned receiving, transmitting, recording, amplifying, information-processing, photographic equipment, tape recorders, televisions, radios, and cameras prohibited from the telecommunications facilities/key distribution center? [CMS 21A, Article 550.j] _____
_____	_____	11. If the COMSEC facility is continuously manned, are security checks conducted at least once every 24 hours? [CMS 21A, Article 550.d(3)(a)] NOTE: Recorded in accordance with local command directives (e.g., line item on watch-to-watch inventory or SF-701). _____
_____	_____	12. In a non-continuously manned COMSEC facility, are security checks conducted prior to departure of the last person and documented using the Activity Security Checklist (SF-701)? [CMS 21A, Article 550.d.(3)(b); SECNAVINST 5510.36, Article 7-10] _____

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES

NO

_____ 13. If a COMSEC facility is in a high risk area and unmanned for periods greater than 24 hours, is a check conducted at least once every 24 hours to ensure that all doors are locked and that there have been no attempts at forceful entry. [CMS 21A, Article 550.d(3)(c)]

NOTE: Recorded in accordance with local command directives (e.g., annotated on SF-702).

_____ 14. Are adequate visitor controls enforced to ensure that access to classified information is given only to visitors who possess the proper identification, security clearance and NEED TO KNOW? [SECNAVINST 5510.30A, Article 11-1, paragraph 2,3; SECNAVINST 5510.36, Article 7-11; CMS 21A, Article 550.e]

_____ 15. Is a visitor's register maintained and retained for one year from the date the register was completed? [CMS 21A, Article 550.e(1)(d)]

_____ 16. Is **unescorted** access limited to individuals whose duties require such access and who meet access requirements? [CMS 21A, Articles 550.e(1)(a)]

_____ 17. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list? [CMS 21A, Article 550.e(1)(b)]

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	18. <u>PART A:</u> Are personnel whose duties require access to COMSEC keying material formally authorized in writing by the CO? [CMS 21A, Articles 450.c, and 505.d]
_____	_____	<u>PART B:</u> If personnel are authorized access to keying material on an access list, has the list been updated annually or whenever the status of an individual changed? [CMS 21A, Article 505.d(2)]
_____	_____	19. Are users of COMSEC material properly cleared to at least the highest level of classified material handled? [CMS 21A, Article 505.a]
_____	_____	20. Is security clearance data for personnel whose duties require access to classified material maintained by the Command Security Manager? [SECNAVINST 5510.30A, Article 9-5, paragraph 2,3,4,5]
		<u>NOTE:</u> For Marine Corps, documented in the Marine Corps Total Force System (MCTFS). For Coast Guard, documented in the Personnel Management Information System (PMIS).
_____	_____	21. Is the COMSEC storage container free of external markings which indicate the classification level of the contents of the security container? [SECNAVINST 5510.36, Article 10-1, paragraph 3]

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES

NO

_____ 22. Do COMSEC storage containers meet the minimum security requirements for the highest classification of material stored therein? [CMS 21A, Article 520.c, 520.d and 520.e; SECNAVINST 5510.36, Chapter 10]

NOTE: Effective 14 April 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized for use to store any classified material. If the LE utilizes a vault for storage, inspect in accordance with Annex C. [CMS 21A, Article 520.f]

_____ 23. Is a Maintenance Record for Security Containers/Vault doors (Optional Form 89) maintained for each security container and retained with the container? [SECNAVINST 5510.36 Article 10-15, paragraph 3, Exhibit 10C; CMS 21A, Article 520.b(3)]

_____ 24. Are all damages, repairs or alterations to the container or parts of the container properly documented on an Optional Form 89? [CMS 21A, Article 520.f; SECNAVINST 5510.36 Article 10-15, paragraph 3]

_____ 25. Is a Security Container Check Sheet (SF 702) maintained for each lock combination of a COMSEC storage container? [SECNAVINST 5510.36 Article 7-10; CMS 21A, Article 520.b(2)]

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	26. Are combinations to COMSEC storage containers changed when initially placed in use, taken out of service, upon transfer/reassignment of personnel who have access, or when compromised? [SECNAVINST 5510.36, Article 10-12; CMS 21A, Article 515.b]
_____	_____	27. Does any one person have knowledge of both combinations to any one TPI container? [CMS 21A, Article 515.c] NOTE: A "Yes" answer on this question constitutes non-compliance. A "No" answer on this question constitutes compliance.
_____	_____	28. Is a Security Container Information Form (SF 700) maintained for each lock combination and placed in each COMSEC storage container? [SECNAVINST 5510.36, Article 10-12, paragraph 3; CMS 21A, Article 520.b(1)]
_____	_____	29. Are sealed records of combinations to COMSEC storage containers maintained in an approved security container (other than the container where the COMSEC material is stored), and available to duty personnel for emergency use? [CMS 21A, Article 515.e]

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES

NO

30. Is each COMSEC material storage container SF-700 record of combination protected as follows: [CMS 21A, Article 515.f]

_____ _____ a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope?

_____ _____ b. Combination envelope sealed using transparent lamination or plastic tape?

_____ _____ c. Name(s) and address(es) of individual(s) authorized access to the combinations recorded on the front of the envelope?

_____ _____ d. Proper classification markings on envelope? [CMS 21A, Article 515.d]

_____ _____ e. Are the envelopes inspected monthly to ensure they have not been tampered with?

_____ _____ 31. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and segregated by status, type and classification? [CMS 21A, Article 520.a(4) and Annex M, Paragraph 3.b]

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES	NO	
_____	_____	32. When not being used and under the direct control of authorized personnel, is all COMSEC material properly stored? [CMS 21A, Article 520.a(2)] _____
_____	_____	33. Are all COMSEC files, records and logs marked, handled and stored in accordance with their highest <u>overall</u> classification? [CMS 21A, Article 715.a] _____
_____	_____	34. Are classified COMSEC files, records and logs annotated with the following statement? [CMS 21A, Article 715.d(2)(c)] "Derived from: CMS 21A Declassify on: X1" _____
_____	_____	35. If the COMSEC facility has keyed crypto equipment from which Top Secret key may be extracted, is the equipment protected under TPI? [CMS 21A, Article 510.d, e] <u>NOTE:</u> See OTAR/OTAT section for key generating equipment _____

ANNEX C

SECTION 1 -- SECURITY (CONT'D)

YES

NO

- _____ 36. Are all COMSEC fill devices loaded with Top Secret key and unloaded COMSEC fill devices in an environment containing keyed crypto-equipment from which Top Secret key may be extracted, being protected under TPI? [CMS 21A, Article 510.d]

NOTE: Review CMS 21A, Article 510.f for exceptions to TPI requirements for fill devices.

SECTION 2 -- LOCAL ELEMENT (USING) RESPONSIBILITIES

- _____ 37. Do all LE personnel have access to written guidance and/or publication extracts (provided by the account EKMS Manager) concerning the proper handling, accountability, and disposition of COMSEC material? [CMS 21A, Articles 455.e, 721 NOTE]
-

- _____ 38. Have all LE personnel who have access to COMSEC material executed a Responsibility Acknowledgement form? [CMS 21A, Article 769.b(2), Annex K]
-

- _____ 39. Do LEs maintain required files (reports, messages, correspondence) as directed by promulgated guidance from the EKMS Manager? [CMS 21A, Article 703 NOTE 2]
-

ANNEX C

SECTION 3 -- LOCAL CUSTODY FILE

YES

NO

- _____ 40. Does the LE's local custody file contain signed, effective local custody documents for each item of COMSEC material held by the LE? [CMS 21A, Article 712]
- _____ 41. Do the local custody documents (i.e., SF 153, or locally prepared equivalent), contain the minimum required information? [CMS 21A, Article 769.c(1)]
- _____ 42. Are local custody documents being maintained on file for 90 days after supersession? [CMS 21A, Annex T, paragraph 2.b]

SECTION 4 -- WATCH STATION INVENTORY/PAGECHECKS

- _____ 43. Does the CONTINUOUSLY MANNED WATCH STATION maintain a watch-to-watch inventory that lists all COMSEC material held (including accountability for resealed segments, STU-IIIs, DTDs and their associated CIKs)? [CMS 21A, Article 775.d(1), Annex AC, paragraph 14.b; CMS-6, Article 310.c]
- _____ 44. Is the material recorded on the watch-to-watch inventory listed by short title, edition, accounting number (as applicable), and quantity? [CMS 21A, Article 775.d(2)]

ANNEX C

SECTION 4 -- WATCH STATION INVENTORY/PAGECHECKS
(CONT'D)

YES	NO	
_____	_____	45. Has the inventory been properly signed and dated for each change of watch? [CMS 21A, Article 775.d(4),(5) and (6)]
_____	_____	46. Are watch-to-watch inventories being retained for 30 days beyond the last recorded date on the inventory? [CMS 21A, Annex T, paragraph 2.k]
_____	_____	47. Have inventories for a NON-WATCH STATION ENVIRONMENT been conducted and recorded on the local custody issue document or a watch-to-watch inventory in accordance with CMS 21A? [CMS 21A, Article 778.c]
_____	_____	48. For NON-WATCH STATION ENVIRONMENTS, are the DTD Supervisory and User CIKs inventoried whenever the account conducts Fixed-Cycle or Combined inventories? [CMS 21A, Annex AC, paragraph 14.a(1)]
		<u>NOTE:</u> The EKMS Manager or Supervisory User may direct more frequent inventories.
_____	_____	49. Are required pagechecks being accomplished in accordance with CMS 21A. [CMS 21A, Article 757, 775.e, 778.d and Annex Y]

ANNEX C

SECTION 5 -- RESEALING/STATUS MARKINGS

YES

NO

- _____ 50. Has all unsealed COMSEC material been sealed/resealed in accordance with CMS 21A and local command instructions? [CMS 21A, Article 772]
-
- _____ 51. Are the effective and supersession dates annotated on all COMSEC keying material, COMSEC accountable manuals and publications in accordance with CMS 21A? [CMS 21A, Article 760.a, 775.g]
-
- _____ 52. Are keytape canisters free of labels (including removal of the NSA applied bar code label) which may conceal penetration or prevent inspection of protective packaging? [CMS 21A, Article 760.e and 760.f]
-

SECTION 6 -- CORRECTIONS AND AMENDMENTS

- _____ 53. Are amendments to COMSEC publications current and properly entered? [CMS 21A, Article 787]
-
- _____ 54. Are corrections to publications made with black or blue-black ink only? [CMS 21A, Article 787.g(1)(b)1]
-
- _____ 55. Is each pen and ink correction identified by writing the amendment or correction number in the margin opposite the correction? [CMS 21A, Article 787.g(1)(b)2]
-

ANNEX C

SECTION 6 -- CORRECTIONS AND AMENDMENTS (CONT'D)

YES

NO

- _____ 56. Has the person entering the amendment signed and dated the appropriate blanks on the publication's Record of Amendments page? [CMS 21A, Article 787.g(2)(a)]
- _____ 57. Has the individual who verified proper entry of the amendment initialed the entry on the Record of Amendments page? [CMS 21A, Article 787.g(5)(b)]
- _____ 58. If pages were removed, substituted, or added; have both the person entering the amendment and the person verifying the amendment conducted a pagecheck of the publication and recorded this on the Record of Pagechecks page? [CMS 21A, Articles 787.g(4) and 787.g(5)(c)]

SECTION 7 -- ROUTINE DESTRUCTION

- _____ 59. Are local destruction records being completed to document destruction of all Top Secret and Secret COMSEC material? [CMS 21A, Article 736.b(2)(b)]
- _____ 60. Are local destruction records being completed to document destruction of all ALC-1 and 2 COMSEC material regardless of classification? [CMS 21A, Article 736.b(2)(c)]

ANNEX C

SECTION 7 -- ROUTINE DESTRUCTION (CONT'D)

YES	NO	
_____	_____	61. Are local destruction records signed or initialed by both personnel conducting the destruction? [CMS 21A, Articles 790.a(5) and 790.f(1)] _____
_____	_____	62. Is destruction of keying material, including zeroizing of fill devices and deletion of key from a DTD, occurring within 12 hours after supersession? [CMS 21A, Article 540.e, 1176, 1177, and Annex AC, Paragraph 15] _____
_____	_____	63. Do local destruction records for segmented COMSEC material contain the following: [CMS 21A, Chapter 7 Fig 7-1, 7-2, 7-3]
_____	_____	a. Short title and complete accounting data? _____
_____	_____	b. Date of destruction? _____
_____	_____	c. Signatures of the two individuals conducting destruction? _____
_____	_____	d. Classification/Declassification markings? "Derived from: CMS 21A Declassify on: X1 _____
_____	_____	e. Marked "CONFIDENTIAL (When filled in)"? _____

ANNEX C

SECTION 7 -- ROUTINE DESTRUCTION (CONT'D)

YES	NO	
_____	_____	64. Is <u>only</u> one copy of a short title, edition, and accounting number recorded on the CMS 25 or locally prepared segmented destruction document? [CMS 21A, Figure 7-1, paragraph 8] _____
_____	_____	65. Can Local Element personnel demonstrate the proper procedures for conducting routine destruction of COMSEC material? [CMS 21A, Article 540 and 790] _____
_____	_____	66. If keying material was unintentionally removed from its protective canister, is the following documentation recorded on its associated disposition record: [CMS 21A, Article 772.d]
_____	_____	a. A statement that the keytape segment(s) were unintentionally removed? _____
_____	_____	b. The date of the unintentional removal? _____
_____	_____	c. Identity of the keytape segment(s) actually removed? _____
_____	_____	d. Signatures of the individuals who removed the key? _____

ANNEX C

SECTION 8 -- DATA TRANSFER DEVICE (DTD)

YES	NO	
_____	_____	67. Is a classification tag attached to the DTD via the lanyard ring to indicate handling requirements when the Crypto Ignition Key (CIK) is <u>not</u> inserted? [CMS 21A, Annex AC, paragraph 8.f]
_____	_____	68. Is a tag attached to the CIK (e.g., via chain) to identify the CIK's classification and serial number? [CMS 21A, Annex AC, paragraph 9.c]
_____	_____	69. For accounts with a Top Secret CIK, is the CIK removed from the DTD and returned to TPI storage when authorized Users are not present? [CMS 21A, Annex AC, paragraph 10.b]
		NOTE: Otherwise, both CIK and DTD must be continually safeguarded according to TPI rules.
_____	_____	70. Is unrestricted access to Supervisory CIKs limited to only those individuals who are authorized to perform all of the associated privileges? [CMS 21A, Annex AC, paragraph 11.d]
_____	_____	71. Does the account ensure that key is <u>not</u> stored on the DTD host side? [CMS 21A, Annex AC, paragraph 12.b]

ANNEX C

SECTION 8 -- DATA TRANSFER DEVICE (DTD) (CONT'D)

YES NO

NOTE: Any known violations of this rule must be reported in accordance with CMS 21A, Chapter 9.

_____ 72. Have recipients of key issued in a DTD, from any source other than a LMD/KP, signed a local custody document acknowledging receipt of the key? [CMS 21A, Annex AC, paragraph 13.c]

_____ 73. Is the DTD audit trail data reviewed by appropriate personnel at least once per month or when the Audit Trail icon illuminates, and these reviews recorded in an Audit Review Log? [CMS 21A, Article 540.c(3)(a) Annex AC, paragraph 17.b, 17.c and 17.d]

_____ 74. Is the Audit Review Log retained at least two years? [CMS 21A, Annex AC, paragraph 17.f(2)]

SECTION 9 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR TRANSFER (OTAT)

NOTE: If a Key Variable Generator (KVG) (i.e., KG-83, KGX-93/93A) is not held, skip to question 77.

ANNEX C

SECTION 9 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR-TRANSFER (OTAT) (CONT'D)

YES	NO	
_____	_____	75. If the COMSEC facility has certified KVG(s) equipment installed for operational use, is the equipment "Dutch Doors" double-locked or protected under no-lone zone (NLZ) procedures? [CMS 21A, Article 1145.k] _____
_____	_____	76. Has the KVG(s) been certified by an authorized facility prior to initial use, every two years thereafter, if security control was lost for any reason and after maintenance/repair? [CMS 21A, Article 1145.b and 1145.c] _____
_____	_____	77. Have NSA-furnished tamper detection labels been applied to certified/recertified KVG(s)? [CMS 21A, Article 1145.h] _____
_____	_____	78. Does each certified KVG have a certification tag on a handle that displays the classification of the equipment, "CRYPTO" status, date of certification, command that performed certification, and name/rank of certifying technician? [CMS 21A, Article 1145.i] _____
_____	_____	79. Have fill devices containing electronic key been clearly labeled (tagged/marked) with the identity of the key it contains? [CMS 21A, Article 1175.b(2)] _____

ANNEX C

**SECTION 9 -- OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR
TRANSFER (OTAT) (CONT'D)**

YES	NO	
_____	_____	80. If the LE generates, transmits, relays or receives electronic key, are local accounting records being maintained? [CMS 21A, Article 1175.b(2) and 1182.d] NOTE: Recipients of key received via OTAR are not required to maintain accounting records. _____
_____	_____	81. If the LE generates electronic key for OTAR and/or OTAT, have accounting records been retained for a minimum of 60 days following the date of the last entry on the key generation log? [CMS 21A, Article 1182.d(1)] _____
_____	_____	82. If the LE relays or receives electronic key (except for receipt of key via OTAR), are local accounting records being retained until the key is superseded? [CMS 21A, Article 1182.d(2)] _____
_____	_____	83. Does the EKMS Manager (or Alternate) conduct a periodic review of OTAT/OTAR accounting logs? [CMS 21A, Article 455.j and 1115.c] _____

ANNEX C

SECTION 10 -- EMERGENCY ACTION PLAN (EAP)

YES	NO	
_____	_____	84. Do all COMSEC users have access to the COMSEC portion of the command's EAP? [CMS 21A, Article 465.1, Annex M, paragraph 2 and 6] _____
_____	_____	85. Are EAP training exercises conducted annually to ensure that everyone is familiar with their assigned duties? [CMS 21A, Annex M, paragraph 6.d(3)] _____
_____	_____	86. For commands, located within the continental United States (CONUS), does the EAP provide guidance detailing actions to be taken for natural disasters, civil/mob actions and terrorism? [CMS 21A, Annex M, paragraph 2.b] _____
_____	_____	87. For commands located outside CONUS, does the EAP provide detailed guidance for both natural disasters and hostile actions? [CMS 21A, Annex M, Paragraph 2.c] _____
_____	_____	88. Have plans been incorporated into the command's EAP to accomplish the following actions during natural disasters: [CMS 21A, Annex M, Paragraph 4] a. Fire reporting and initial fire fighting by assigned personnel? _____
_____	_____	b. Assignment of on-the-scene responsibility for protecting COMSEC material held? _____

ANNEX C

SECTION 10 -- EMERGENCY ACTION PLAN (EAP) (CONT'D)

YES	NO	
_____	_____	c. Protecting material when admitting outside fire fighters into the secure area(s)? _____
_____	_____	d. Securing or removing classified COMSEC material and evacuating the area(s)? _____
_____	_____	e. Assessing and reporting probable exposure of classified COMSEC material to unauthorized persons during the emergency? _____
_____	_____	f. Completing a post-emergency inventory of COMSEC material and reporting any losses or unauthorized exposures to appropriate authorities? _____

SECTION 11 -- EMERGENCY DESTRUCTION PLAN (EDP)

NOTE: The questions in this section apply only to LEs that are located outside CONUS or are onboard a mobile platform that deploys outside CONUS.

_____	_____	89. Does the LE have an Emergency Destruction Plan (EDP) incorporated into its EAP? [CMS 21A, Annex M, Paragraph 2.g, 2.j and 2.k] _____
-------	-------	--

ANNEX C

SECTION 11 -- EMERGENCY DESTRUCTION PLAN
(EDP) (CONT'D)

YES	NO	
_____	_____	90. Does the EDP identify personnel assignments and the chain of authority that is authorized to make the determination that emergency destruction is to begin? [CMS 21A, Annex M, Paragraph 5.d(5) and 5.d(6); SECNAVINST 5510.36, Exhibit 2B PART II paragraph 4]
_____	_____	91. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [CMS 21A, Annex M, Paragraph 5.d and 6.c]
_____	_____	92. Are the sensitive pages of KAMs prepared for ready removal (i.e., upper left corner clipped), and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [CMS 21A, Annex M, Paragraph 5.e(2)(a)]
_____	_____	93. Are the priorities of destruction indicated in the plan? [CMS 21A, Annex M, Paragraph 8]
_____	_____	94. <u>Is the EDP divided into two parts: one for precautionary and one for complete destruction?</u> [CMS 21A, Annex M, Paragraph 7]

ANNEX C

SECTION 11 -- EMERGENCY DESTRUCTION PLAN
(EDP) (CONT'D)

YES

NO

- | | | |
|-------|-------|--|
| _____ | _____ | 95. Does the EDP provide for the adequate identification and rapid reporting of the material destroyed, to include the method and extent of destruction? [CMS 21A, Annex M, Paragraph 10] |
| <hr/> | | |
| _____ | _____ | 96. Does the EDP stress that accurate information concerning the extent of emergency destruction is second in importance only to the destruction of the material itself? [CMS 21A, Annex M, Paragraph 10.a] |
| <hr/> | | |
| _____ | _____ | 97. Are document sinking bags available in sufficient quantity and in good condition to permit jettison of COMSEC material?
(NOTE: Surface units only)
[CMS 21A, Annex M, Paragraph 9.d(2)(b)] |
| <hr/> | | |
| _____ | _____ | 98. If User deploys in aircraft, does the plan cover specific actions to be followed in aircraft? [CMS 21A, Annex M, paragraph 9.c] |
| <hr/> | | |

<p style="text-align: center;">ANNEX D INSPECTION GUIDE VAULT</p>
--

PURPOSE. To provide a checklist (with appropriate references) for use by personnel tasked with certifying/recertifying a vault which is used for storage of COMSEC material to ensure it meets the minimum physical security safeguards.

INITIAL, REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

Immediate Superior in Command (if other than EKMS Inspector) of Unit Inspected:

Date of Last Inspection: _____

Name/Grade/Rate and Command of Inspector:

Date of Last Facilities Approval: _____

EKMS Manager Name/Grade: _____

Primary Alternate EKMS Manager Name/Grade: _____

Identify Following, as Applicable/Assigned:

Second Alternate EKMS Manager Name/Grade: _____

Third Alternate EKMS Manager Name/Grade: _____

<p style="text-align: center;">ANNEX D INSPECTION GUIDE VAULT</p>
--

ACTION. The following inspection checklist shall be used and completed, in it's entirety, by the Inspector conducting the inspection. Per Chapter 2 and Article 401.c., inspection reports evaluated as unsatisfactory must include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to respond to any questions that receive a negative response. This inclusion in the inspection checklists will greatly aid inspectors and commands when conducting the out-brief and writing the official report of inspection results.

- - - - -

VAULT CHECKLIST

YES NO

1. For **class "A" vault**, (authorized for storage of **TOP SECRET and below** keying material, are the following constructed properly and with approved materials? [CMS 21A, Annex N, Paragraph 2]

- | | | |
|--------------|--------------|---|
| <p>_____</p> | <p>_____</p> | <p>a. <u>Floors and walls</u>: 8 inches of reinforced-concrete to meet current structural standards. Wall shall extend to the underside of the roof slab.</p> <p>_____</p> |
| <p>_____</p> | <p>_____</p> | <p>b. <u>Roof</u>: Monolithic reinforced-concrete slab of a thickness to be determined by structural requirements, but not less than the walls and floors.</p> <p>_____</p> |

ANNEX D

VAULT CHECKLIST (CONT'D)

YES NO

- ___ ___ c. Ceiling: The roof or ceiling shall be reinforced concrete of a thickness to be determined by structural requirements, but not less than the walls and floors.

NOTE: Where the existing roof does not conform to the vault roof requirements stated above, a vault roof, which is structurally equal to the vault walls shall be constructed.

- ___ ___ d. Vault Door and Frame Unit: Shall conform to Federal Specifications AA-D-2757, Class 8 vault door, or Federal Specification AA-D-00600 (GSA-FSS) Class 5 vault door.
-

- ___ ___ e. Lock: A combination lock that conforms to the Underwriters' Laboratories, Inc. Standard No. 768, for Group 1R or Group 1. The specific lock model used shall bear a valid UL Group 1R or Group 1 label.

NOTE: All vault doors procured after 14 April 1993 must be equipped with a GSA-approved combination lock that meets the requirements of Federal Specifications FF-L-2740.
[CMS 21A, Annex N, paragraph 2]

2. Are COMSEC storage vaults equipped with the following minimum safety requirements:
[CMS 21A, Annex N, paragraph 5.a]

- ___ ___ a. A luminous type light switch? (**NOTE**: May be painted with fluorescent paint.)
-

ANNEX D

VAULT CHECKLIST (CONT'D)

YES NO

- ___ ___ b. Is emergency lighting installed?

- ___ ___ c. An interior alarm switch or device?
(e.g., telephone, intercom)

- ___ ___ d. A decal containing emergency instructions on
how to obtain release if locked inside the
vault?

3. If an emergency escape device **is** considered
necessary, have the following minimum requirements
been met: [CMS 21A, Annex N, paragraph 5.b]
- ___ ___ a. Is it permanently attached to the **inside** of
the door and can not be activated by the
exterior locking device, or otherwise
accessible from the outside?

- ___ ___ b. Is it designed and installed so that drilling
and rapping the door from the outside will
not give access to the vault by activating
the escape device?

- ___ ___ c. Has the device met the requirements of GSA
Federal Specification AA-D-00600 (GSA-FSS)
paragraph 3.3.9, dated 27 December 1963,
concerning an exterior attack on the door?

ANNEX D

VAULT CHECKLIST (CONT'D)

YES NO

4. If an emergency escape device **is not** provided, have the following approved Underwriters Laboratories (UL), Inc., devices been installed in the vault: [CMS 21A, Annex N, paragraph 5.c]

___ ___ a. A UL Bank Vault Emergency Ventilator?

___ ___ b. At least one UL approved fire extinguisher situated in a position near the vault door?

NOTE: These provisions are recommended even if an emergency escape device is provided.

___ ___ 5. Are emergency destruction tools available? [CMS 21A, Annex M, paragraph 5.d and 6.c]

___ ___ 6. Is the space/compartment or vault which contains COMSEC material outwardly identified as "RESTRICTED AREA"? [OPNAVINST 5530.14C, Article 0319.d, Appendixes VI and VII]

___ ___ 7. Is a central record of combinations maintained in a security container, approved for storage of the highest classification of the material protected by the combination locks, for each vault used for the storage of COMSEC material? [CMS 21A, Article 515.e]

ANNEX D

VAULT CHECKLIST (CONT'D)

YES NO

- ____ 8. If the original security integrity of the vault has been degraded in any way, have approved repairs been made? [SECNAVINST 5510.36, Article 10-15]

NOTE: Effective 01 April 93, commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are no longer authorized to store any classified material. [CMS 21A, Article 520.f]

9. Does the vault door unit include a day gate which conforms to the following: [CMS 21A, Annex N, paragraph 3]

NOTE: This is not a requirement, but is highly recommended.

- ____ a. Is the gate of the swing-in hinge type with vertical rods not less than 1/2 inch diameter?
-

- ____ b. Is the gate frame made of not **less than** 3/8" by 1 1/2" steel members, and equipped with a locking device arranged to permit locking and unlocking of the gate from the inside?
-

ANNEX E
INSPECTION GUIDE
FIXED COMSEC FACILITIES

PURPOSE. To provide a checklist (with appropriate references) for use by personnel tasked with certifying/recertifying a fixed COMSEC facility which contains classified COMSEC material, located in an immovable structure or aboard a ship, to ensure it meets the minimum physical security safeguards.

INITIAL, REQUIRED DATA:

Date of Inspection: _____

Command Inspected: _____

Immediate Superior in Command (if other than EKMS Inspector) of Unit Inspected: _____

Date of Last Inspection: _____

Name/Grade/Rate and Command of Inspector: _____

Date of Last Facilities Approval: _____

EKMS Manager Name/Grade: _____

Primary Alternate EKMS Manager Name/Grade: _____

Identify Following, as Applicable/Assigned:

Second Alternate EKMS Manager Name/Grade: _____

Third Alternate EKMS Manager Name/Grade: _____

Clerk Name/Grade: _____

<p style="text-align: center;">ANNEX E INSPECTION GUIDE FIXED COMSEC FACILITIES</p>
--

ACTION. The following inspection checklist shall be used and completed in its entirety by the Inspector conducting the inspection. Per Chapter 2 and Article 401.c., unsatisfactory inspection reports must include references and comments to substantiate the evaluation. As such, below each item reviewed, space is provided to respond to any questions that receive a negative response. This inclusion in the inspection checklists will greatly aid inspectors and commands when conducting the out-brief and writing the official report of inspection results.

FIXED COMSEC FACILITY CHECKLIST

YES NO

- | | | |
|--------------|--------------|--|
| <p>_____</p> | <p>_____</p> | <p>1. Is the facility constructed of solid, strong materials that deter and detect unauthorized penetration? [CMS 21A, Annex O, paragraph 2]</p> <hr/> |
| <p>_____</p> | <p>_____</p> | <p>2. Does the facility provide adequate attenuation of internal sounds that would divulge classified information through walls, doors, windows, ceilings, air vents, and ducts? [CMS 21A, Annex O, paragraph 2]</p> <hr/> |
| <p>_____</p> | <p>_____</p> | <p>3. Are walls constructed from true floor to true ceiling? [CMS 21A, Annex O, paragraph 3.a]</p> <hr/> |
| <p>_____</p> | <p>_____</p> | <p>4. Are ceilings at least as thick as the outer walls and offer the same level of security as the outer walls? [CMS 21A, Annex O, paragraph 3.b]</p> <hr/> |

ANNEX E

FIXED COMSEC FACILITY CHECKLIST (CONT'D)

YES NO

- ____ 5. If false ceilings are used, are additional safeguards used to resist unauthorized entry (e.g., installed, approved intrusion detection system (IDS) in the area above the false ceiling)? [CMS 21A, Annex O, paragraph 3.c]
-
- ____ 6. Is only one door used for regular entrance to the facility, though other doors may exist for emergency exit and entry or removal of bulky items? [CMS 21A, Annex O, paragraph 4]
-
- ____ 7. Do all doors remain closed during facility operations and are they only opened to admit authorized personnel or materials? [CMS 21A, Annex O, paragraph 4.a]
-
8. Do the main entrance facility doors comply with the following standards: [CMS 21A, Annex O, paragraph 4.b(1)(a) through (c)]
- ____ a. Does the door have sufficient strength to resist forceful entry? (In preference order, examples of acceptable doors are: GSA-approved vault doors, Standard 1-3/4" internally reinforced, hollow metal industrial doors, or metal-clad or solid hardwood doors with a minimum thickness of 1-3/4").
-

ANNEX E

FIXED COMSEC FACILITY CHECKLIST (CONT'D)

YES NO

- ____ ____ b. Is the door frame securely attached to the facility and fitted with a heavy-duty/high security strike plate, and hinges installed with screws long enough to resist removal by prying?
-
- ____ ____ c. Is the door installed as to resist removal of hinge pins? (This can be accomplished by either installing the door so that the hinge pins are located inside the facility, or by set screwing/welding the pins in place.)
-
- ____ ____ 9. If the facility is not continuously manned, is the the door equipped with a GSA-approved, electro-mechanical lock meeting Federal Specification FF-L-2740? [CMS 21A, Annex O, paragraph 4.b(2)]
-
- ____ ____ 10. If the facility is continuously manned (a built-in lock is not required), is the door designed so that a GSA-approved, electro-mechanical lock meeting Federal Specification FF-L-2740 and dead bolt can be affixed to the outside should it ever become necessary to lock the facility? (e.g., in case of emergency evacuation.) [CMS 21A, Annex O, paragraph 4.b(2)(a)]

NOTE: An electronically activated lock (e.g., cipher lock or keyless push-button lock) may be used on the entrance door to facilitate the admittance of authorized personnel when the facility is operationally manned. However, these locks do not afford the required degree of protection and may not be used to secure the facility when it is not manned.

ANNEX E

FIXED COMSEC FACILITY CHECKLIST (CONT'D)

YES NO

- ___ 11. Do other doors (e.g., emergency exit doors and doors to loading docks) meet the same installation requirements as the main facility entrance doors, and designed so that they can only be opened from inside the facility? [CMS 21A, Annex O, paragraph 4.b(3)]

NOTE: Approved panic hardware and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility.

- ___ 12. Is the entrance area equipped with a device which affords personnel desiring admittance the ability to notify personnel within the facility of their presence? [CMS 21A, Annex O, paragraph 4.b(4)]
-

- ___ 13. Is a method employed to establish positive visual identification of a visitor before entrance is granted? [CMS 21A, Annex O, paragraph 4.b(4)(a)]
-

- ___ 14. Is the entrance designed in such a manner that an individual cannot observe classified activities until cleared for access into the restricted spaces? [CMS 21A, Annex O, paragraph 4.b(4)(b)]
-

- ___ 15. Where windows exist, are they secured in a permanent manner to prevent them from being opened? (COMSEC facilities normally should not normally contain windows.) [CMS 21A, Annex O, paragraph 5]
-

ANNEX E

FIXED COMSEC FACILITY CHECKLIST (CONT'D)

YES NO

- ___ 16. Are windows less than 18 feet above ground alarmed and/or barred to prevent their use as an access point? [CMS 21A, Annex O, paragraph 5.a]
-
- ___ 17. Is observation of internal operations of the facility denied to outside viewing by covering the windows from the inside, or otherwise screening the secure area from external viewing? [CMS 21A, Annex O, paragraph 5.b]
-
- ___ 18. Are other openings such as air vents, ducts, or any similar openings which breach the walls, floor, or ceiling of the facility, appropriately secured to prevent penetration? [CMS 21A, Annex O, paragraph 6]
-
- ___ 19. Do openings which are less than 96 square inches, have approved baffles installed to prevent an audio or acoustical hazard? [CMS 21A, Annex O, Paragraph 6.a]
-
- ___ 20. If the opening exceeds 96 square inches, are acoustical baffles supplemented by either hardened steel bars or an approved intrusion detection system (IDS)? [CMS 21A, Annex O, paragraph 6.b]
-

ANNEX F

EKMS INSPECTION REPORT EXAMPLE

From: (EKMS Inspector)

To: (ISIC/IUC)

Subj: REPORT OF EKMS INSPECTION OF (COMMAND TITLE)

Ref: (a) EKMS 3A

1. Title of command inspected: _____
EKMS ID number: _____
Date inspected: _____
Inspected by: _____
(Name, Rank/Rate/Grade)
EKMS Inspector Certification: _____
(Date Certified/Re-certified)
Certifying ISIC: _____
Certifying A&A Team: _____

2. Evaluation of the command or unit inspected, [GRADE: (SAT or UNSAT)] and comments as required to substantiate the evaluation.

3. Findings:

a. List each finding/discrepancy which is significantly important to require action. Cite the appropriate reference(s) for each finding/discrepancy noted. Do not list items of a minor administrative nature.

b. Immediately below each finding, list and briefly discuss any corrective actions recommended to resolve the discrepancies listed above.

4. Any additional comments or remarks.

5. The facility meets all physical security standards and continued approval to hold classified COMSEC material up to the level of _____ is authorized.

6. [In accordance with reference (a), copies of this report, portions thereof, or correspondence related thereto, from a source external to the Department of the Navy shall include the appropriate caveat included in EKMS 3A, either Article 410.a., 410.b., or 410.c.]

I. M. SALTY
(EKMS Inspector)

ANNEX F

EKMS INSPECTION REPORT EXAMPLE (CONT'D)

Copy to:
(Commands as indicated by the ISIC)

***** DO NOT FORWARD COPIES TO DCMS *****

ANNEX G

EKMS FEEDBACK REPORT EXAMPLE

FM (ISIC/IUC)//OFFICE CODE//
TO DCMS WASHINGTON DC//80//
INFO COMNAVCOMTELCOM WASHINGTON DC//N34//
CHAIN OF COMMAND
UNCLAS //N02201//
MSGID/GENADMIN/(ORIG ISIC/IUC PLA)//
SUBJ/EKMS FEEDBACK REPORT//
REF/A/DOC/DCMS/OCT98//
AMPN/EKMS-3A, EKMS INSPECTION MANUAL, ARTICLE 405//
POC/I.M. SALTY/ITCS(SW)/-/-/DSN:321-7654//
RMKS/1. ISIC INSPECTOR'S RECOMMENDATION(S) FOR CHANGES TO
EKMS INSPECTION POLICY AND/OR PROCEDURES. IF APPLICABLE
PROVIDE SUPPORTING DOCUMENTATION.//
BT